Middle-East Journal of Scientific Research 15 (8): 1120-1124, 2013
ISSN 1990-9233
© IDOSI Publications, 2013
DOI: 10.5829/idosi.mejsr.2013.15.8.11536

# Cybercrimes: Concept and Problems of Terminology

[1]*Aratuly Kuanysh and* [2]*Bostanbekov Kairat*

[1]Kazakh National University named after Al-Farabi, Kazakhstan
[2]Kazakh National Technical University named after K.I. Satpaev, Kazakhstan

**Abstract:** In Kazakhstan society there is a stereotype that commission of crimes with working of the computer equipment-event unique to only foreign countries and because of a weak computerization of our society, that is inconclusive introduction in industrial and social relations of information technologies, absent at all. This instance also resulted in absence some serious scientific researches of this problem. Computer and information technologies function relatively long ago and their development trigger huge temps that is connected with a big interest in the people at large. The crimes coming from working of the computer equipment-it is only specialized part of criminal activity in the information sphere. This category appertains and the crimes, commission of which is illegal access to computer information protected by law. Within the last 15-20 years as far as the computerization of economic and administrative and financial and commercial activity appear new types of crimes which began to be called computer, by reference from terminology of foreign legal practice.

**Key words:** Cybercrimes · Information · Computer · Information technologies · Hackers · Terminology · Computer systems · Information security · Networks

## INTRODUCTION

According to informal facts,one of the earliestserious banking computer crime occurred during a course of three years beginning in 1970. The chief teller at the Park Avenue branch of New York's Union Dime Savings Bank embezzled over $1.5 million from hundreds of accounts [1, 150]. The first crime of this kind in the former USSR was registered in 1979 in the city of Vilnius. This case was a certain starting point in development and research of a new type of crimes.

Gradually before our eyes there was an information industry, whose independence and prospective development every whit depended on exact regulation of the legal relationship incipient of formation and using of information resources. "Information revolution" has overtaken the country during the difficult economic and political period and demanded urgent regulation of problems incipient on its way. Meanwhile, as we know, legal mechanisms can be included and become effective only when the public relations sufficiently stabilized.

Information became a principium of life of modern society, a subject and a product of its activity and process of its creation, accumulation, bailment, transfers and processings in turn stimulated progress in the field of tools of its production: electronic and computer technologies, telecommunication facilities and networking. All this as a whole enters into concept of definition of new information technology which policies and resort of implementers of information processes in various areas of human activity, that is way of realization of information activities of the person who can also be considered as information system. Information turns into a product of the public relations, starts procure becomes a purchase and sale subject.

One of types of information technologies is the computerization. The supposition of a world computerization as specifies B.H.Toleubekova, was informational explosion of the middle of the XX century, the demanding systematization, regulating of stored knowledge, creation of a databank, storages for more extending list of information from the most various branches of human activity. There are an objective necessity for equipment which would take on itself the lion's share of this work. And such equipment was created in the form of computers or as they were called, electronic computing machines (ECM) [2,10].

**Corresponding Author:** Aratuly Kuanysh, Kazakh National University named after Al-Farabi, Kazakhstan

The beginning of the 90th years of the XX century in Kazakhstan, as well as on all the former Soviet Union, was marked by the beginning of a universal computerization of spheres of human activity. Initially computers began to be applied in the bank sphere, further at full peltbecamecome to life the computerization of educational institutions,are instantiateddatebases in computers law enforcement agencies.

However new information technologies stimulated not only society and state progress, but also emergence, and coming into existence and development of earlier negative processes.

As far asimplementation of information technologies to various spheres of life of society the problem of fight against computer crimes become aggravated. In foreign countries with high level of a computerization it became for a long time an one of paramount. Domestic and foreign publications and pocket mass media of the last years with the various concepts, designating these or those new hospitalities of criminal character in information area.Granting of enough visible contours of such social and legal phenomenon as what crimes in global computer networks act, in the theory still there is no generally accepted legal definition. But some definitions of the phenomenon could be found in literature, for example: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"[3, 6].In literature it is possible to meet a number of concepts («computer crimes», «crimes in the sphere of high technologies», «communication crimes», «cybercrimes», «crimes in the sphere of computer information», «information crimes», «cybergangsterism», «network crimes»), generally meaning the same types of criminal activity. Foreign researchers more often use such concepts, as high-techcrime, by cybercrime, networkcrime which are respectively translated as «crimes in the sphere of high technologies», «cybercrimes», «crimes in computer networks». In the majority of sources foreign authors use terms «cyber crime» and «computer crime» as the same[4, 2]. Criminals are called by «hackers», «crackers», «cyberpunks», «bandits on information superhighways».

So, A.V.Dulov carries to computer crimes «the various crimes committed by means of computers, with violation of their activity» [5,1]. It seems to us, similar definition is quite wide and containing essential inaccuracy: fruition of computer crimes not necessarily must beviolation activity of the computers themselves. Public dangerous consequences can come and at normal functioning of the firmware of the computer on condition of incorrect basic data, at mistakes of the operator or the programmer, at thefts of machine time, illegal access, etc.

N.A.Selivanov carries to computer crimes, the crimes which subject is computer information or as which means of commission the electronic computer facilities used for the purpose of commission of illegal offence of other object [6,37]. Disproving this point of view, V.V. Krylov [7,4] considers that approach according to which in the legislation it is necessary to reflect concrete technological tools, doesn't justify itself and therefore is inadvisable to accept the term «computer crimes» as a basis for the name in criminalistics of all set of crimes in the field of informational relapses. The computer, in his opinion, is only one of varieties of information equipment and problems of use of this equipment don't settle set of the relations connected with the circulation of confidential documentary information. B.B. Krylov suggests to consider as the basic concept «information crimes», recognizing that the developed system of legal relationship in the field of information activities allows to abstract from concrete technical means. It draws a conclusion that crimes in the field of the computer information, UK allocated in separate chapter, are part of the information crimes united by the general instrument of information processing-the computer.

Yu.M.Baturin divides objects of computer attacks to three categories [8,9]: computers, objects which can be attacked by means of the computer as the tool, objects for which the computer is an environment. It seemsfounded not to include in structure of objects of computer crimes the first category on this classification in cases when computers are no more than property, to absolutely equivalent any other material things and aren't pertain to allocation in separate legal category only on the basis of their name.

The classical point of view about that computer crimes can be limited to use of the COMPUTER as the tool (tool) and an endeavor subject, N.F.Akhramenka adheres to the classical point of view also. Thus specifies that the computer can't be considered as a subject of computer crimes as «a subject of endeavors at their commission is at all the equipment as that (the damage, as a rule, isn't caused to it) and information stored, processed or transferred by this equipment. Defining object of computer endeavors, we recognize that crimes such with the much bigger basis it is necessary to carry to information» [9,23]. In our opinion, the subject of computer crimes should be expanded even more: besides information to include still normal functioning of computer facilities and information processes.

Undoubtedly, this list of opinions isn't exhaustive, however it is important not: it is necessary to distinguish crimes in the sphere of high information technologies and so-called computer crimes. Unfortunately, the last term so strongly became current scientific and practical workers as in Kazakhstan and abroad that became already traditional and some authors believe that it is hardly worth changing it, «as many names in timeacquire conditional character».

Distinction in terminology indicates not only concern of society about new threat, but also absence of full understanding of an essence of this threat. It is important that terminological inaccuracy of a statement of the law or the methodological recommendation about its execution can entail its wrong application and , therefore and negative consequences.

It should be noted that the conventional definition of the crime committed with use or concerning computer equipments, computer information, the software, isn't available today, in general, the criminal law of the foreign states covers this concept various in character and degrees of public danger types of illegal acts.

To a question of criminalization of offenses in the sphere of high information technologies today in the world there are three approaches.

The first consists in reference to crimes of unauthorized access to the protected computer systems, infections with viruses, illegal use of computer systems and information. It is characteristic for such countries, as Norway, Singapore, Slovakia, Philippines, South Korea.

The second approach consists in recognition by computer crimes of only those acts which are connected with causing damage to property and electronic information processing (Austria, Denmark, Sweden, Switzerland, Japan). For example, in the legislation of Austria, Denmark, criminal liability for unauthorized intervention in functioning of information systems is provided.

The third approach is characteristic for the countries with high level of a computerization (the USA, Great Britain, France, Germany, the Netherlands) and the developed legal base. It consists in criminalization of the acts connected not only with property damage, but also with violation of the rights of the personality, with threat of national security etc. So, from the content of norms of criminal law of Great Britain follows that its sanctions are applied to «the law breakers caused by means of the COMPUTER damage or using information in the purposes». In the 80th years the system of criminal justice of Germany offered a number of criminal and legal definitions of studied category of illegal acts.

The criminal police of this country in the sphere of high technologies refers to crimes «all illegal actions at which electronic information processing is the tool of their commission and (or) their object».

One of the most developed cybercrime legal base could be seen in the USA. Cybercrime laws in this country are devided in two groups: Substantive cybercrime laws (e.g., laws prohibiting online identity theft, hacking, computer systems, child pornography, intellectual property, online gambling, totally 20 laws) and Procedural cybercrime laws (e.g., authority to preserve and obtain electronic data from third parties, including internet service providers; authority to intercept electronic communications; authority to search and seize electronic evidence, totally 3 laws)[10,2]

It should be noted that similar crimes are even more often committed by the staff of firm, bank or other establishment which finally and to be caused damage. For example, in the USA the computer crimes committed by employees, make 70-80% of the annual damage connected with computers. In Kazakhstan there is such tendency too. So, in 2000 in London citizens of Kazakhstan on a charge ofnot authorized computer penetration, plot, harming by extortion and harming attempt by extortion with use of corporate information of the «Bloomberg LP Company» were arrested. The sum of blackmail made 200 thousand dollars. They were arrested at the airport at the time of transfer of money. It is noteworthy is that, working in the company making databases for «Bloomberg LP», they used information received during it for achievement of the criminal purpose. The trial of them took place only in the summer of 2002, proceeding from complexity of proof of such crime. In the USA where passed judicial proceedings, the maximum term of punishment on set for these crimes makes about thirty years.

The problem of information security really exists and is constantly aggravated as a result of penetration practically in all fields of activity of society of technical means of processing and data transmission. But it is impossible to lose sight and other objects of criminal legal protection. In this regard it would be effectually to include in set of the crimes forming computer crime, not only crimes in the sphere of computer information, but also those crimes at which commission the computer information being on the machine carrier is exposed to illegal influence. It is caused, first of all, by that computers found broad application practically in all spheres of human activity.

In practice often difficult happens to distinguish the crimes encroaching on safety of computer information and the crimes committed with use of the computer as means of commission of crime. Their difference consists, first of all, in object of encroachment. Object of the crimes encroaching on safety of computer information, the condition of security of information being on the machine carrier, in the COMPUTER, system of the COMPUTER or their network, from the illegal access which is carried out to it and also from negative impact of harmful programs and violation of the rules of use by electronic computer facilities. In the crimes made with use of the computer equipment, as object that public relation on which concrete encroachment is directly directed acts. For example, at fraud with as use of the computer equipment by direct object the property relations act, at radio-electronic espionage-external safety and the sovereignty of the Republic of Kazakhstan.

However both in those and in other cases encroachment of object of a crime is carried out by means of impact on a subject of a crime as which the computer information being on the machine carrier acts.

Thus, being based that up to the present moment in science isn't developed somecommon classification model of crimes, it very difficult to make as it is necessary to consider multi-purpose aspect of similar classifications [11,70]. Computer crime as independent type of crime and definition of groups of the crimes forming computer crime, it is necessary to consider as an integrating sign the computer information being on the machine carrier influence on which carries out the perpetrator at commission of crime.

All this gives the grounds to define computer crime as set of crimes at which commission influence is carried out on the computer information being on the machine carrier. On the way of such association investigative practice also. So, in separate law enforcement agencies of the Republic of Kazakhstan special divisions which are engaged in investigation of the crimes entering into group of computer crime are created, without dividing them on objects of encroachment. Expediency of such association locates, on the one hand, that at investigation of similar crimes special technical knowledge for carrying out investigative actions is required and with another-uniformity of precautionary measures of these crimes.

So, in 2003 in the Republic of Kazakhstan Management on the organization of fight against crimes in the sphere of information technologies of Committee of criminal police of the Ministry of Internal Affairs of Republic of Kazakhstan which activity is directed on was created:

- fight against crimes in the sphere of computer information (the COMPUTER, their systems and a network, thus the rights of the owner of information also are object of criminal encroachment);
- fight against crimes in the sphere of telecommunications (the COMPUTER, their systems and a network are the tool of commission of crimes);
- fight against the crimes encroaching on constitutional laws of citizens (inviolability of private life, secret of correspondence, telephone negotiations, post, cable or other messages);
- fight against crimes against moral (pornography distribution, Internet procurement, a child pornography);
- fight against crimes in the sphere of economic activity (illegal use of the trademark, a fake of license products, production or sale of counterfeit payment cards, etc.);
- direct realization of the international obligations in the field of struggle against crimes in the sphere of high technologies (actualization of operational coordination with foreign law enforcement agencies according to messages on transnational computer and telecommunication crimes, an exchange of urgent information, inquiries and execution of search tasks in formats of member countries of «Eight» and the Interpol).

Today, implement the tasks assigned to it, Management «K», reached significant results in improvement of methods of fight:

- with offenses in the market of intellectual property, the timely prevention and the detection of offenses, connected with illegal production, distributions and uses of objects of copyright and the allied rights. The employees the persons who are engaged in a fake of license products-movies on DVD, the software, CD disks come to light. Divisions «K» actively interact with security services, lawyers and technicians of the enterprises and the organizations;

- with crimes on networks of telecommunications. According to «Rules of interaction of government bodies and the organizations at introduction and operation of hardware-software and technical means of carrying out operational search action on networks of telecommunications of the Republic of Kazakhstan», carry out removal, interception of the criminal information used further in the course of proof on criminal cases. We believe that by these rules it is regulated not only possibility of implementation of actions on information removal, but also the probability of carrying out system of the actions directed on detection, fixing, research and use in proof of the obtained electronic data is defined;
- with crimes in the bank sphere. Counteraction of legalization of money and other property, got by a criminal way by means of high technologies is carried out.

## REFERENCES

1. Weitzer, R., 2003. Current Controversies in Criminology. Upper Saddle River. New Jersey: Pearson Education Press, pp: 15.
2. Toleubekova, B.H., 1995. Computer crime: yesterday, today, tomorrow: Monograph. Karaganda: KVSh GSK RK, pp: 1-320.
3. Moore, R., 2005. Cyber crime: Investigating High-Technology Computer Crime. Cleveland, Mississippi: Anderson Publishing, pp: 1-68.
4. Halder, D. and K. Jaishankar, 2011. Cyber crime and the Victimization of Women: Laws, Rights and Regulations. Hershey: PA, USA, pp: 1-54.
5. Dulov, A.V., 1992. Criminalistic analysis of computer crimes. Problems of computer crime, Scientific research institute PKKSE MU RB (issue 2), pp: 3-4.
6. Selivanov, N.A., 1993. Problems of fight against computer crime. Legality, 8: 37.
7. Krylov, V.V., 1998. Information as element of criminal activity. NewsMoskow university, 4(Ser. 11.Right): 50-64.
8. Baturin, Y.M., 1990. Computer crime. Right and informatics, Moscow State University, pp: 9.
9. Akhramenka, N.F., 2001. Criminalization of socially dangerous behavior with use of information computation systems. M, pp: 1-160.
10. Cybercrime Laws of the United States “Al Rees, CCIPS” of October 2006. Computer Crime and Intellectual Property Section, U.S. Department of Justice.
11. Chufarovsky, Y.V., 2004. Criminology in questions and answers: Textbook. M: TK Velbi, Prospect, pp: 1-270.