Criminal Acts in Computer Systems and their Legal Regulation

Darius Štitilis
Legal informatics department, Law academy of Lithuania, Vilnius, Lithuania
dstitilis@mwe.lt

Rimantas Petrauskas
Legal informatics department, Law academy of Lithuania, Vilnius, Lithuania
rpetraus@ita.lt

Abstract
The present work deals with some legal regulation problems of criminal acts in computer systems. The use of computers and spreading of computer technologies in almost all areas of life has created a lot of legal problems. One of the main problems is a new kind of acts, not yet regulated by criminal law in some states. The legal problems of computer-related crimes in computer systems are discussed in this article. The legal situation related to criminal acts in computer systems in Lithuania is discussed too.

Keywords: criminal law and computer systems, computer crimes

1. Introduction
Development of information society relies on widespread use of computer systems and computer networks. Computer systems are used to store confidential social, economic or personal data and perform many other functions. But burgeoning of computer systems has, however, a negative side: it gave start to antisocial and criminal behavior in the ways that would never be possible otherwise. Persons and organizations suffer huge damage from those criminal acts. Various scientists started to discuss those problems. Legal regulation of criminal deed in computer systems became urgent. However, legal regulation of this activity in Lithuania is not sufficient yet. Thus, the purpose of the article is to discuss more widely criminal acts in computer systems and their legal regulation in foreign countries and in Lithuania.

The advent of computer technology has brought many kinds of opportunities and some of these, surprisingly, are of criminal nature. Computers may facilitate commission of "old-fashioned" crimes such as fraud or counterfeiting or give rise to new mischief such as computer hacking and the erasure of programs of data.

There are no precise, reliable statistics on the amount of computer crime and the economic loss to victims, partly because many of these crimes are apparently not detected by victims, many of these crimes are never reported to authorities, and partly because the losses are often difficult to assess. Nevertheless, there is a consensus among both law enforcement personnel and computer scientists who specialize in security that both the number of computer crime incidents and the sophistication of computer criminals is increasing rapidly.

2. Classification of criminal acts
The development of information technologies reveals the emergence of new types of interests which call for legal protection, especially as regards the integrity of computer systems and data. The Council of Europe has made important contributions to specifying the types of conduct that should be penalized.
From 1985 to 1989, the Select Committee of Experts on Computer-Related Crime of the Council of Europe discussed the legal problems of computer crime. The Committee elaborated a report, which was adopted by the European Committee on Crime Problems at its 38th Plenary Session in June 1989. The Select Committee of Experts on Computer-Related Crime and of the European Committee on Crime Problems prepared Recommendation No. R (89) which was adopted on 13 September 1989 at the meeting of the Ministers' deputies.

This Recommendation suggests that, when reviewing their legislation or initiating new legislation, the Member States governments take into account the report on computer-related crime and in particular the so-called "guidelines for the national legislatures" [1; 157]. These guidelines for national legislatures include a "minimum list" and "optional list".

The minimum list of acts, which the Council of Europe recommended to treat as crimes if committed intentionally, is as follows:

1. "Computer Fraud": The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing that influences the result of data processing thereby causing economic or possessor loss of property of another person (Alternative draft: with the intent to unlawfully deprive that person of his property.) with the intent of procuring an unlawful economic gain for himself or for another person.
2. "Computer Forgery": The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence.
3. "Damage to Computer Data or Computer Programs": The erasure, damaging, deterioration or suppression of computer data or computer programs without right.
4. "Computer Sabotage": The input, alteration, erasure or suppression of computer data or computer programs, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system.
5. "Unauthorized Access": The access without right to a computer system or network by infringing security measures.
6. "Unauthorized Interception": The interception, made without right and by technical means, of communications to, from and within a computer system or network.
7. "Unauthorized Reproduction of a Protected Computer Program": The reproduction, distribution or communication to the public without right of a computer program which is protected by law.
8. "Unauthorized Reproduction of a Topography": The reproduction without right of a topography protected by law, of a semi-conductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semi-conductor product manufactured by using the topography.

The guidelines of the Council of Europe also identify, in an “optional list” the following additional areas that could be criminalized, if committed intentionally:

1. "Alteration of Computer Data or Computer Programs": The alteration of computer data or computer programs without right.
2. "Computer Espionage": The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person.
3. "Unauthorized Use of a Computer": The use of a computer system or network without right, that either: (a) is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or (b) is made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or (c) causes loss to the person entitled to use the system or harm to the system or its functioning.

4. "Unauthorized Use of a Protected Computer Program": The use without right of a computer program which is protected by law and which has been reproduced without right, with the intent, either to procure an unlawful economic gain for himself or for another person or to cause harm to the holder of the right" [2].

The threat and extent of criminal acts in computer systems and the need for penal regulation is shown in 1996 survey conducted by the Federal Bureau of Investigations and Computer Security Institute. Of 428 organizations questioned, 42% claimed to have been victims of computer-related crime in the last 12 months. The combined estimated losses from these crimes ranged from 145$ million to 730$ million over the one year period. The survey indicates that a big threat to computer systems comes from employees: more than 50% of those 42% reported that the threat was from inside. The larger computer fraud ever attempted, which concerned the transfer of 70$ million, involved one employee of First National Bank of Chicago [3; 223]. To combat those activities, it is very important to develop criminal law related to the activities in computer systems.

In perhaps one of the most comprehensive studies of the United Nations Commission on Crime and Criminal Justice results show that 72% of the respondents reported a security incident within the previous 12 months, with 43% reporting the incident of criminal nature [4; 223]. The threat of criminal acts related to computer systems grows when such acts are directed to computer systems performing many functions, upon which human life depends. Medical treatment and air traffic controls are two examples.

In England, the Computer Misuse Act 1990 (CMA) was enacted dealing with criminal activity related to computers. The act filled the loopholes in the prior law. In particular, it created three new offences:

1. Unauthorized access to computer material (section 1);
2. Unauthorized access with intent to commit or facilitate commission of further offences (section 2);
3. Unauthorized modification of computer material (section 3).

Sections 1 and 2 of the act are designed to outlaw the gaining of unauthorized access to computer-held programs or data, whether by an outsider acting remotely ("hacking"), or an insider, such as a company employee, gaining access to computer-held material which he or she has no permission to see [5; 267].

Section 1 creates the summary offence:

1. (1) A person is guilty of an offence if –
   a) he causes computer to perform any function with intent to secure access to any program or data held in any computer;
   b) the access he intends to secure is unauthorized, and;
   c) he knows at the time when he causes the computer to perform the function that that is the case.

The term’s “program” and “data” within section are left undefined by the Act. These terms were left undefined for fear of a definition becoming outdated due to technological developments [6; 214].

Section 3 creates an offence of doing any act which causes unauthorized modification of the contents of any computer with the requisite intent and knowledge as defined by the section.
3 of the CMA 1990 appears to be capable of catching a wide variety of types of activity. It should also be capable of covering the intentional introduction of viruses, worms, Trojan horses\(^1\) and other programs of a potentially destructive nature [7; 353]. The very first case under the Computer Misuse Act 1990 that of *R v Cropp* raised questions about the scope of the Act. Cropp was charged with an offence under s 2(1) (which requires the establishment of an offence under s 1(1)) following an incident which occurred when he visited the premises of his ex-employer, a wholesaler, with his new employer. Cropp showed interest in an item, picked up machine and a salesperson bagman to enter the details on the storeroom computer. The salesperson was called away during this operation and Cropp, being well acquitted with the operation of the system took the opportunity to input a discount of 70%. His new employer subsequently paid invoice for £204.60 plus VAT of the correct sum of £710.96 plus VAT [7; 349].

English scientists think CMA is very effective weapon to combat criminal activities in computer systems.

There are several United States laws or sections of laws that apply specifically to computers and computer-related crimes. There are others in which certain sections have been interpreted to cover computer technology. In addition to these U.S. federal laws, many states have adopted their own computer crime laws. Computer-related crimes can be charged under at least forty federal statutes. One of them – "Computer Fraud and Abuse Act" (CFAA): in 1986, USA Congress passed a federal law outlawing some of the activities related with computer systems. The statute represented a complete rewriting of a 1984 statute, which proved inadequate to the task of dealing with the problem of computer crime.

The statute criminalizes six types of computer activities:

1. the unauthorized access of a computer to obtain information of national secrecy with an intent to injure the United States or advantage a foreign nation;
2. the unauthorized access of a computer to obtain protected financial or credit information;
3. the unauthorized access into a computer used by the federal government;
4. the unauthorized interstate or foreign access of a computer system with an intent to defraud;
5. the unauthorized interstate or foreign access of computer systems that results in at least $1000 aggregate damage;
6. the fraudulent trafficking in computer passwords affecting interstate commerce.

Each of these provisions also require proof that the defendant accessed the computer without authorization or, in the case of the use of a computer with the intent to defraud, that the defendant exceeded his authorization to access the computer.

As is apparent from this list of offences, some activities in computer systems can result in a violation of the CFAA. Although the most obvious offences seem to require malicious intent, the law has also been applied in situations where the perpetrator's criminal intent was not clear [7; 108].

According to U.S. legal regulation by penal law, many illegal acts in computer systems are punishable.

---

\(^1\) A virus is a self-replicating program which not be immediately apparent on examination of a system but copies itself into the computer memory and from there to any disks which are subsequently loaded and/or into the memory of other computers attached to the same network as data is exchanged. Worm is an example of a program that was developed of exploring the capabilities of computer systems and networks and may adversely affect systems on which it is unwanted by consuming resources. A Trojan horse is a program which appears as a program performing an innocuous function but hides the fact that it also has another, usually more sinister, function.
3. Development in Lithuania

Development of the Lithuanian criminal law related to activity in computer systems is not sufficient. It is necessary to stress that the valid penal law does not include enactment (typical to some developed countries) where computer crimes are straight formulated. However, the amendments of the penal law have brought several novelties: at the moment the Criminal Code of Lithuania has some specific definitions of criminal acts in computer systems, covered by traditional crimes:

1. Article 135-2. Intentional influence on computer information and its processing [8]. (this activity is related to influence on election or referendum results).
2. Article 274. Fraud (this activity related to formation of knowingly incorrect computer program, recording of incorrect data in computer memory etc.).
3. Article 277. Causing damage to property by deception or breach of trust (this activity is related to formation of knowingly incorrect computer program, recording in computer memory of incorrect data etc.).

But such legal regulation is not sufficient since there is no separate section, according to UN Recommendation '89, related to criminal activities in computer systems. But there are prepared two separate drafts of the Criminal Code. The first one, prepared by the Ministry of Justice, does not have separate provisions related to computer crimes. According to the draft, illegal activity related to computers should be qualified by general rules. The second one (preparatory work leader V.Piesliakas, judge of the Supreme Court of Lithuania, professor) has a separate section of provisions related to computer crimes:

Section 33. Information security crimes.
Article 335. Destruction or modification of a computer information.
Article 336. Destruction or modification of computer program.
Article 337. Theft of information [9].

Will these new articles cover all criminal acts in computer systems? But it seems that some criminal acts, mentioned in EU R'89, do not fall into the effect sphere of section 33. For example, a person who knowingly accesses computer system without authorization but does not obtain any information, according Section 33, is innocent.

The lower level of computerization in Lithuania than in the developed countries and the small number of reported cases explains why no particular attention was earlier paid to the topic of criminal activity in computer systems. Even a definition has not been developed. Scientists and lawyers have mostly dealt with the presentation of the experience of other countries in order to bring the problem attention.

4. Conclusion

The penal laws of developed countries include enactment where computer crimes are straight formulated. Lithuanian criminal laws developments in that area are not sufficient. Lithuanian academicians, governmental bodies, information technology professionals should promote the implementation of UN’89 Recommendations so that criminal law addresses the new challenges of information technologies. The academic and scientific community, as well as governments, should undertake further research concerning criminal acts in computer systems. Such research should in particular examine the incidence of such activity, the extend of losses, the methods of commission and the characteristics of offenders.
5. References


