Actions of Corroboration of Felony in IT Crime in Legislation of the Republic of Serbia with a Retrospect of International Standards

Aladin Semovic[1], Milos Babovic[2], Aladin Madzovic[1], Dzemail Zornic[3]

[1]*Basic Court in Novi Pazar, Serbia*
[2]*University of Montenegro, Law Faculty, Podgorica, Montenegro*
[3]*University in Novi Pazar, Serbia*

Abstract **– Computer crime represents an international issue which all democratic societies, including ours, need to stand against. Accordingly, it is necessary to introduce such legal definitions in positive legislation of the Republic of Serbia which take into account the specificity of electronic proof, in order to use collected proof as valid in a court procedure. Also, an international standardization of process rules of a criminal procedure regarding actions of corroboration of this kind of crime is necessary, in order to use proof collected in a foreign state through an international legal cooperation in criminal matters in our state, and vice versa, having in mind trans-national component of IT crime.**

Keywords - actions of corroboration, IT crime, electronic proof.

1. Introduction

In this paper we will deal with the issue of corroboration actions for criminal acts against security of computer data, what legal solutions are accepted in our positive legislation, and we will try to point out to the needs of amending and adding to them. We will make a restrospective of international standards in the field and necessity of updating legislation of the Republic of Serbia with international conventions.

Before we start discussing the issue, it is neccesary to make a short retrospective of what has been adopted in he criminal legislation of the Republic of Serbia with the goal of fighting against IT crimes.

With regard to criminal material law, we can say that a major breakthrough has been made with the introduction of special group of criminal acts against security of computer data into the Criminal Law („Official newsletter of RS“ no.85/05, 88/05, 107/05, 72/09).The following criminal acts have been identified:Damaging computer data and programs(art.298), Computer sabotage(art.299), Production and launch of computer viruses (art.300), Computer fraud (art.301), Unauthorized access to a protected computer, computer network and electronic data processing (art.302), Preventing and limitng access to a public computer network(art.303), Unauthorized use of computers or computer networks (art.304) andProduction, procurement and giving to other people funds to commit criminal acts against security of computer data (304a).

A major breakthrough has been made in organizational law as well. With the Law on organization and jurisdiction of state authorities for the fight against high-tech criminal („Official newsletter of RS“ no.61/05 i 104/09) „one defines establishment, organization, jurisdiction and authorization of special organizational units of authorities for discovering, prosecution and legal action for criminal acts defined by this law“

However, in the field of criminal process law, very little has been done, especially with corroboration actions.We think this link is extremely important in suppressing this kind of crime, having in mind the complexity of issue before us, so it is necessary to introduce certain amendments and additions to the Law on criminal procedure („Official newsletter ofSRJ“ no.70/01;68/02; „Official newsletter of RS“ no.58/04, 85/05, 115/05, 49/07, 20/09, 72/09).

2. Specificness of electronic proof

A special importance for proving criminal acts in computer crimes and other crimes commited through computers goes to electronic evidence.

Electronic evidenceis information or data of relevance for investigation, stored or transferred through a computer. The mentioned evidence has the same value as all other material evidence and the rules regarding it are the same as for all other evidence. However, one cannot lose from sight the specificity of electronic data which comes from their nature, their sensitivity to change, erasure od destruction.Also, electronic evidence can be stored on an individual computer, computer network or a

remote server outside territorial jurisdiction of collecting authorities,they can be visible or invisible, which, beside their susceptibility to change or destruction either willingly or unintentionally, imposes specificity in their collecting.This very specificity of electronic evidence which comes from its nature can have a great impact on determining facts, which are vital in pre-legal procedure, police work and the prosecutor's work and in the investigation phase, conducted by a judge. [1].

Generally, in digital forensics of computer system, potential sources of digital evidence can be found in hardware and program components of a system:

- HD, magnetic tape, external/removable storage devices
- log files of network infrastructure (*firewall, IDS/IPS, proxy* server)
- applications and log files of security-relevant events (audit clues)
- e-mail,
- contents of other servers (Windows files, web servers, databases etc)
- recorded network traffic[2].

3. Corroboration actions in current criminal–process legislation of the Republic of Serbia

In accordance with the acting Law on Criminal Procedure, the following actions of corroboration are proscribed : Searching an apartment and a person(art.77-81), Temporary requisition of an object (art.82-86), processing suspicious items(art.87-88), Questioning a defendant (art.89-95), Questioning a witness (art.96-109), Inspection(art.110-112), Fact-finding (art.113-132) i Photography or sound and video recordings(art.132a).

Of all the above mentioned corroboration actions, only the article 89 §2 of the Law on Criminal \procedure (Temporary requisition of an object) proscribes special authorization and mechanisms of governmental agencies to collect evidence for felony in computer crimes. Thus, it is proscribed to enlist devices for automatic data processing and equipment for storing electronic data as objects "which in accord with the Criminal Law are to be seized or which can serve as evidence in a criminal procedure. A person using these devices and equipment is obliged to enable access to them to an authorized agency, upon an order from the court, and to provide information as to their use. Before requisition of these items, an agency implementing the procedure will inspect them in presence of an expert and maintain a log of them. If the user is present, he or she can enter a note."

Other actions of corroboration are related to all criminal acts, regardless of the group they belong to. Within them, there are no specific authorizations of governmental agencies relating specifically to IT crimes, a huge handicap in our opinion, bearing in mind specificity of electronic evidence.

4. Special investigation techniques in the current criminal-process legislation of the Republic of Serbia

In chapter XXIXa of the Law on Criminal Procedure, special codes have been proscribed on procedure for organized crime, corruption and hard crimes. There are codes related to measures of agencies in discovering and proving these criminal acts, among which are : 1) Surveillance and recording phone and other communications (art.504e-504z), 2) Providing simulated business services and providing simulated legal jobs(art.504i-504k), 3) Controlled delivery (504l), 4) Automatic computer search of personal and related data (art.504lj); as well as codes relating to special measures of prosecuting agencies for discovering and proving criminal acts from art.504a §.3of this law: 1) Under-cover investigator and 2) Protected witness.

However, these special investigation techniques and measures have remained beyond reach of special governmental agencies for the fight against high-tech crime, for they are applicable only for criminal acts stated in art.504a of the Law on Criminal Procedure, where the criminal acts against security of computer data are not stated.

These legal solutions are in our opinion unacceptable and need urgent change. However, to make paradox even worse, new Law on Criminal Procedure ("Official Newsletter of RS" 72/11, 101/11), in art.162 §.3.proscribes that only one special corroboration action–Secret communication surveillance from art.166 can be used for some criminal acts from the field of high-tech crime and that is for : "Unauthorized use of copyright or items of related law (art.199 of CL), Damaging computer data and programs (art.298.§.3.ofCL),Computer sabotage(art.299.ofCL),Computer fraud(art.301.§.3.of CL) and Unauthorized access to a protected computer, computer network and electronic database(art.302.of CL)".

What is new is that with search actions, by the art.152 §3 of the new LCP, it is proscribed that "search of devices for automatic processing of data and equipment where electronic data are stored or can be stored is conducted with an order from the court and with the expert help", whereas the current LCP does not deal with this issue.

5. Necessity of conforming legal solutions of the Republic of Serbia with international legal framework

International coordination and cooperation are as significant as legal frameworks. Laws on high-technology crimes by themselves can gain little without help from internal governmental structures and trained personnel necessary for effectvie solving of jurisdiction issues, international help requests, search and requisition of evidence. Computer crime represents one of the most complex and urgent cases in international cooperation [3].

It is clear that a coordinated and constant approach to foreign assistance is necessary with investigations and criminal prosecution so that the clues of electronic crime could be traced across time zones and areas of legal jurisdiction, with different legal systems and levels of technical preparedness. [3].

The most significant international legal act relating to the fight against computer crime is the Convention on Cyber Crime, passed by European Council in Budapest on November 23, 2001. In part 2 of the convention – Procedural Law, the member states are ordered to "pass such legislative and other necessary measures to establish those authorizations and procedures which are proscribed in this section, with the aim of implementing certain criminal investigations and procedures" Those are: 1) Expositive conservation and protection of stored computer data, 2) Expositive conservation and protection and partial disclosure of transfer data, 3) Issuing order, 4) Search and requisition of computer data, 5) Collecting computer data in real time, 6) Intercepting data in electronic communications.

Beside the above mentioned convention, there are numerous international acts dealing with this issue. One of them is the Recommendation of the Council of Europe R (95) 13, dealing with the issue of procedural law regarding IT.

It is especially important that in the attachment of this Recommendation there are the rules on search and temporary requisition related to information systems, intercepting information sent through the systems, extended investigation, technical surveillance and cooperation of people who have the computer devices with investigating agencies, with the obligation of removing or decrease the impact of passwords. [4].

Electronic evidence is required to be provided in the manner that it can be used as evidence in national and international proportions. Therefore the manner of providing evidence must be in accord in international proportions, and that means starting with international rules and recommendations [4].

We can find examples of good legal solutions originating from adjustment of positive national rules with international legal standards in the neighboring countries.While reviewing the Croatian Law on Criminal Procedure, („National News", no. 152/08, 76/09 i 80/11), we come to conclusion that the legislator of the country paid special attention to this growing issue and set a good framework for national agencies to get special authorizations and mechanisms to subjugate computer crime in proper manner.

Thus, within action of collecting evidence – search, there is a special enactment (art.257) which regulates search of computers and other devices, as well as obligations of their users and telecommunications providers regarding access and providing necessary information during the searches. Also, within collecting evidence - temporary requisition of an item, there is an enactment (art.263) relating to „data stored in computers and related devices, devices that serve for collecting and transmitting data, data carriers and subscriber information which the provider possesses". It is proscribed that „when collecting, recording, protecting, and storing data, one shall especially take care of regulations relating to secrecy of certain data". Unlike Law on Criminal Procedure of Serbia, the art.332of the Law on Criminal Procedure of Croatia, numerous evidence actions are proscribed which can be enacted for felonies in article 334, including acts in computer crime and some other acts perpetrated through use of computers or networks.As a special action, interception, collecting and recording of computer data is proscribed. In the end, one should mention that art.331 proscribes electronic (digital) evidence as evidence action.

Similar legal solutions related to corroboration actions – search and temporary requisition of items, as well as attitude to application of special investigation techniques, are accepted in Law on Criminal Procedure of Bosnia and Hercegovina (Official newsletter no. 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07 i 9/09), aswell as in Law on Criminal Procedure of Montenegro (Official Newsletter no.57/09).We have to admit that enactments of Croatian Law on Criminal Procedure are more precise, which makes it easier for them to be interpreted and applied, having in mind specificity of evidence material.

We will here look at art.83 § 1 and 2 of the Law on International Legal Assistance in criminal matters of the Republic of Serbia („Official Newsletter" of RS, no.20/09), which enlists into other forms of international legal assistance „application of measures such as surveillance, and recording of phone and other ways of communicating, optical recording of people, controlled delivery, providing

simulated business services, providing simulated legal jobs, hiring a special under-cover investigator, computer search and data processing".However, according to enactments of the current Law on Criminal Procedure of the Republic of Serbia, it is not possible to apply these measures for criminal acts against security of computer data, so for the sake of better cooperation on internatonal level and conformity with international standards, we propose amendments to the Law on Criminal Procedure which will enable special investigation techniques for criminal acts in the field of computer crimes.

6. Relationship between privacy right and corroboration actions

The privacy right, being a fundamental human right, is widely recognized in various documents on human rights. In art.12 of Universal Declaration on Human Rights it is stated: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks". Likewise, art 8. Of the European Convention of Human rights proscribes: „Everyone has the right to respect for his private and family life, his home and his correspondence"[3].Only under strict supervision of state authorities can one order search and requisition for gathering evidence material.

Constitution of the Republic of Serbia („Official Newsletter"of RS, no.98/2006)by article 40, foresees inviolibality of home, where: „No one may without the written decision of the courtenter a person's home or other premises against the will of their tenant nor conduct a search in them", unless„it is necessary for direct imprisonment of a perpetrator or removing direct and serious danger for people or property, in the way stipulated by law". By article 41 of the Constitution of RS, inviolability of letter secrecy and of other means of communication is guaranteed, and „ aberrance is allowed for only certain periods and on the basis of court decision, if necessary for managing a criminal procedure or protection of security of the Republic of Serbia, in the way stipulated by the law".

While studying enactments of the current Law on Criminal Procedure, we cannot find their grounding in the Constitution. That is, enactments proscribed in article 77-81 of the LCP do not treat searching device for electronic data processing or computer equipment, and article 85 of the LCP, which proscribes temporary requisition of letters, telegrams and other items, never mentions electronic mail nor it can be concluded from them. However, we witness a great number of cases where, when searching is done by authorities, then computers and other equipment are requisitioned and processed, it is done against the law. Thus, we have a double violation of human rights, first by computer criminals, then by governmental agencies investigating the crimes.

7. Conclusion

International cooperation is a key factor in fighting against these criminal offences, and without conforming domestic regulations with international standards regarding application of corroboration actions and special investigation techniques, such cooperation is impossible. It is therefore necessary to confirm domestic law with international framework as soon as possible, so that computer criminals would not use our country as a place where they can perpetrate these offences without being punished accordingly.

The development of computer technology has hugely enhanced ability for tracking and surveillance of individuals and their behaviour. Therefore the issue of legal protection of citizen data is being stressed, especially in functioning of administrative agencies. It is necessary to find true measure between freedom protection and civil rights on one hand and the need of the community to ensure public interest is safe, on the other one [5].

References

[1]. Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, *Priručnik za trening tužilaca i sudija u oblasti visokotehnološkog kriminala*, www.uts.org.rs, *downloaded on 14.04.2012.god.*

[2]. Milosavljević, Milan &Grubor, Gojko, *Istraga kompjuterskog kriminala (Metodološko –tehnološke osnove),* Univerzitet Singidunum, Beograd, 2009.

[3]. Džodi R., Vestbi, Međunarodni vodič za borbu protiv kompjuterskog kriminala, Beograd, 2004.

[4]. Pavišić, Berislav, KomentarZakona o kaznenom postupku, Dušević&Kršovnik doo, Rijeka, 2011.

[5]. Ištvan, Feješ, Savremeni kriminalitet i dokazno pravo, Novi Sad, 2002.

[6]. Zornić Dž., *Kompjuterski kriminal, zločin i prevencija,* Beograd 2010, konferencija ZITEH10 *http://www.singipedia.com/content/1073-kompjuterski-kriminal.pdf*

*Corresponding author:**Aladin Semovic***
*Institution: **Osnovni sud u Novom Pazaru***
*e-mail:**aladinsemovic@gmail.com***