TACTICAL RULES USED TO HEAR OFFENDERS IN THE CASE OF CYBERCRIMES

Adrian-Cristian MOISE*

Abstract

The paper presents and analyses some of the forensic tactics used by investigators in cybercrimes hearing procedures.

Since cybercrimes have a cross-border character, investigators must use both notions in the field of forensic tactics, as well as notions in the field of information and communication technology.

Keywords: *cybercrimes; forensics; investigator; tactical rules*

JEL Classification: [K 14]

1. Introduction

Given the particularities of committing cybercrime, the hearing of the suspect or defendant person must be carefully prepared, taking into consideration the perspective of a psychological dispute between the investigator and the offender in order to establish the truth, the existence or not of the criminal offence.

The active subject of cybercrime is an individual, often with an advanced training in the field of computer science, which makes it difficult to investigate cybercrime.

2. Prepare the hearing of offenders in the case of cybercrimes

2.1 Studying existing materials or data

The study of the material of the cause, as well as the whole preparation of the hearing, is carried out with maximum *emergency* and *promptness*, the dominant tactical rule in trying to solve cases with cybercriminals.

On the forensic tactical plan, the study of the case materials involves knowing the data on the manner and circumstances in which the deed was committed, the evidence existing at that time on the file, the participants, the

* Associate Professor, PhD., "Spiru Haret" University of Bucharest, Faculty of Juridical, Economic and Administrative Sciences, Craiova, Romania; Attorney-at-law, Dolj Bar, Romania.

injured person, witnesses, data to be completed, confirmed or also verified by the cyberspace offender's statements (Stancu, Moise, 2014, p. 237).

2.2. Knowing the personality of the cybercrime offender

This tactical requirement has a direct, immediate impact on the establishment of listening tactics, serving to further outline the subjective side of cybercrime.

The main elements that lead to defining the personality of the cybercrime offender are the following: the personality traits, such as the character, the temperament and the skills; the factors that have influenced or conditioned the somatic and mental evolution (speech, walking) and social evolution of cybercrime offenders, such as the family or social environment in which he/she evolved and formed, the circle of friends, the level of intelligence, the possible criminal antecedents, relationships with other participants in cybercrimes or with the victim.

All this data can be obtained from the study of the material of the cause, from the information gathered from the workplace, from the domicile, from the witness statements, from the investigation of the criminal record, as well as from the preliminary discussions with the cybercrime offender.

2.3. Drawing up the hearing plan

The preparation to hear the cybercrime offender will materialize in a *hearing plan*, drawn up for each individual offender. It will contain the problems to be clarified and the succession of their approach, the background or detail questions to which the heard offender will have to answer, the materials that will be presented to him/her.

The planning of the hearing must be of a flexible nature, which will also lead to the possibility of adapting, modifying or formulating new questions about the investigated deed and the person of the author of the cybercrime offence (Stancu, Moise, 2014, p. 239).

2.4. Organization of the way to conduct the hearing of cyberspace offenders

The interrogation mode falls within the general criminal prosecution plan drawn up in a particular criminal case and which contains the versions, the problems to be clarified, the tactical methods used, the order of carrying out the various procedural activities, as stated above.

From a tactical point of view, the organization of the hearing involves: accurately establishing the problems to be clarified at the hearing, as well as the data to be verified on this occasion; preparing the evidence material to be used during the hearing, such as, for example, material means of evidence,

photographs, various recordings; determining the order in which the hearing will be made, so that if there are more cybercrime offenders, there will at first be heard those who have more data, or those who make honest and complete statements; establishing the summoning modality, the date, the time and the place where cybercrime offenders are to be present for the hearing; the order and the modality of summoning must be conceived so as to avoid, at least in the first hearing phase, the contact between the various persons concerned, especially in the case of several suspects or defendants, witnesses, injured parties, civil parties.

3. Actual hearing of the cybercrime offenders

According to the provisions of the Articles 107-110 of the Romanian Criminal Procedure Code, the hearing of the cybercrime offender is carried out in three main stages: checking the identity of the cybercrime offender, the hearing of the cybercrime offender in the free account phase and in the asking questions phase, followed by the recording of statements.

At this time, previously prepared, they proceed to the direct application of the forensic tactical rules of hearing, depending on the particularities of each type of cyber offender, on the personality of the person being heard.

It is necessary that all persons on the spot be identified and heard one after the other, whether they are eyewitnesses, perpetrators, injured persons, representatives of injured individuals or legal entities, other persons who know the data of interest for the investigation, in order to clarify certain problems, such as (Moise, 2011, p. 232-233):

- the identity of the owner and of the persons entitled to operate in the information system and with data relevant to the investigation of offenses against data and information systems;
- passwords and other ways of crossing access barriers;
- the purpose in which the information system is used;
- devices, programs, tools used to secure the computer system, for data destruction or hiding, or scheduled self-destruction;
- use of the information system for purposes other than those authorized by law or contract;
- measures taken to secure the space in which IT systems operate;
- persons with tasks related to the prohibition of access to and abuse operation of information systems and how they have performed their tasks;
- the main threats to the security of computer systems and data that have been the subject matter of the illicit activity;
- identifying hidden folders by a special program; these folders are only visible after typing certain keys, entering certain passwords, etc.

- any explanatory documentation relating to the hard disk or software installation system;
- other events or indications of suspicion encountered in the operation of the information system.

During the on-site investigation in the case of cybercrimes or computer search, if the cybercrime offender is present, the prosecution must prevent any access of him/her to the computer system. Especially, if the cybercrime offender has a superior IT training, he may wilfully alter the data on his/her computer system, without the investigators being aware of it.

The suspect's computer system may contain some commands that can cause the data loss, commands that can be concealed under the name of some usual commands of the operating system used.

From people present at the on-site investigation and at the computer search or from other people who are familiar with the operation of the computer system, important information can be obtained. Each witness should be interviewed on how seized computer systems are used (Pintea, 2005: 35). Data entry, sorting and storage methods on the computer, as well as practices related to various aspects of its current use are relevant.

In some special situations, the computer systems of other people located in the same location may have relevant evidence. For example, there are cases where relevant documents were found in the IT systems of the secretaries of the investigated persons.

2. 4. Tactical procedures used in hearing of the cybercrime offenders

The determining role in the choice of tactical procedures is represented by the position of the computer offender against the accusation brought to him, by the attempts to dissimulate the truth and his/her psychic structure.

In the assumption of recognition and of sincere and complete statements, no special tactical problems are raised, the questions referring only to some clarifications or additions. In the case of the cybercrime offender's refusal to make statements, the judicial body must, through the tactical procedures used, find out the reason for the refusal and try to persuade him/her to give up this attitude.

Difficulties arise in the case of false, incomplete, contradictory statements, in the case of rejecting the accusation, persisting in refusing to make statements or returning with new elements to previous statements. In these cases, the hearing tactics acquire a very complex character.

The forensic tactics has developed some tactical hearing procedures, procedures whose effectiveness has been demonstrated by the positive practice of judicial bodies.

The following tactical procedures are known in the literature (Stancu, 2011, p. 234-236):

- Repeated hearing

The tactic of the repeated hearing is used, in particular, for incomplete, contradictory and misleading statements.

This process consists of repeatedly hearing of the cybercrime offender about the same facts and circumstances, about the same details. Taking place at certain time intervals, there will inevitably be contradictions, inconsistencies, inaccuracies between statements of the cybercrime offender, with all the attempts to reproduce those previously reported.

The details cannot always be set, they cannot be repeated, with all the preparations made in this respect by the heard offender. Thus, these contradictions must ultimately be explained by him/her, thus demonstrating the unsubstantiated nature of his/her previous affirmations, being thus determined to recognize the truth.

- Cross-hearing

The tactic of cross-hearing consists in questioning the cybercrime offender by two or more investigators at the same time. This procedure, which aims at breaking down the defence system of the investigated one, which is in the position of total negation of the committed deed. The advantage is that the cybercrime offender is not given the opportunity to prepare false answers, the questions being addressed by each investigator alternately at a sustained and alert pace.

In order for this tactical interrogation procedure to be effective, the position occupied by the two investigators must be front and side left or right and slightly backwards so that they are not visually observed by the cybercrime offender, causing it not only to listen to the question, but to return to the sound source, which contributes to the disorganization of the defence.

A variant of cross-hearing is the successive hearing by two persons. Both tactical procedures are based on the idea that cybercriminals may become more communicative towards one of the investigators.

Through this procedure, the accused person/defendant is asked through the questions to systematically clarify how he conceived and prepared the offence, who were the participants and how they acted, etc. If the suspect/defendant has committed several crimes in relation to his/her personality and psychology, the criminal investigation body will determine whether or not the hearing will begin in relation to the simplest or the most serious crime.

When there are more cybercrime offenders, each should be heard both on their own activity and separately on each participant's activity.

- Systematic hearing

This method is used in the case of the honest cybercrime offender to help clarify all the problems of the cause, especially in complex cases with a high degree of difficulty, as well as in the case of the cybercrime offenders who are insincere, refractory, to compel them to give logical, chronological explanations, successive in all aspects of the offence charged.

Within this procedure, through the questions, cybercrime offenders are asked to systematically clarify how they conceived and prepared the offense, who were the individuals involved, and how each of them acted.

- Tactic of surprise meetings

The tactic of surprise meetings is used in the case of the plurality of cybercrime offenders and becomes effective if it is used in psychic moments of a certain tension, created specifically to obtain sincere statements.

The procedure consists on asking some questions to cybercrime offenders after they saw one of the accomplices being entered in a room next door.

- Using detail questions

As the name implies, this procedure quantifies some aspects of the statements made by free account, nuancing them to be more rigorous, more credible.

From the judicial practice we can conclude on the efficiency of the procedure especially for cybercrime offenders with criminal experience who present themselves before the investigators with the statements previously prepared, in the sense that they repeat until the stereotyping of the statements they will give in the interrogation.

- Using evidence of guilt

It is an investigation strategy almost exclusively distributed to the insincere cybercrime offender who uses all his or her possibilities or those involuntarily offered by the investigator to distort the truth and make it difficult to investigate to escape criminal liability.

This type of cybercrime offender recognizes only the deeds committed when they are convinced of the reasonableness of the evidence that accuses him/her.

Conclusions

In order for the hearing of cybercrime offenders to take place under normal circumstances, the investigators need to know very well the characteristics of the cybercrime offenders' personality.

Knowing the personality of the offender in the cyberspace is important for identifying measures to prevent and combat the cybercrime phenomenon.

The study of the personality of the cybercrime offender involves an approach to all the social factors that determine and influence the criminal

behaviour in the virtual space as well as the psychic characteristics of the offender in cyberspace.

Each offense committed in the cyberspace has a particular peculiarity to be considered, and the possibility of committing a crime is determined by a series of personality traits that are influenced by factors such as the offender's age and sex, certain mental disabilities, etc.

The main components of cybercrime offender's personality structure are the following (Fedushko, Bardyn, 2013, p. 57): biological and hereditary factors; the closest social environment, which refers to the family and socio-economic status of its members, to the particularities of children's education, to school, to attitudes towards learning process, to relationships with teachers and classmates, to the friends and their social status, to the values and the status of the child in a group of friends; personal and psychological characteristics, such as the character traits and the temperament, the sphere of motivational value, the level of claims, self-esteem and possible conflicts in this field, the relation regarding the chosen profession, the understanding of the motivation for choosing the profession, the place of the chosen profession in the system of values of the society, future plans; the level of awareness of the legal regulation on the conduct of activities in the online environment.

Bibliography

1. Fedushko S.; Bardyn, N., (2013), *Algorithm of the cyber criminals identification*, în Global Journal of Engineering, Design & Technology, Global Institute for Research & Education, Volume 2, No. 4, July-August 2013. Retrieved 31st of January 2019 from: http://www.gifre.org/gjedt/gjedtbackissues.aspx.
2. Moise, A.C., (2011), *The forensic investigation methodology of cybercrimes*, Bucharest: Universul Juridic.
3. Pintea, Al., (2005), *Elements of forensic tactics in the investigation of cybercrimes*, Romanian Journal of Forensic Science no. 1.
4. Stancu, E., (2011), *Tactical procedures used in criminal investigations. Developments*, Bucharest: AIT Laboratories SRL.
5. Stancu, E., Moise, A.C., (2014*), Criminalistics. Technical and tactical elements of criminal investigation*, second edition, Bucharest: Universul Juridic.
6. The Romanian Criminal Procedure Code.