Considerations on the use of technical surveillance in criminal proceedings

Stancu ȘERB, Ph.D
,,Alexandru Ioan Cuza" Police Academy, Bucharest
stancuserb@yahoo.ro

Petre UNGUREANU, Ph.D
Police Inspectorate of Brasov County, Romania,
Service of Criminal Investigations

Abstract: *The use of technical surveillance in criminal proceedings refers to interception of communications or any kind of remote communications, access to a informatics system, audio-video surveillance, tracking and locating by technical means and obtaining data on a person's financial transactions. The use of technical surveillance binds the criminal investigation body to fulfill all the necessary conditions stipulated by the law, such as proportionality and subsidiarity principles, an on-going investigation regarding an offense stipulated in art. 139 par. 2 of the Criminal Procedure Code. The judicial bodies must always consider the balance that must exist between the achievement of a criminal investigation and the respect for right to privacy, family, private and postal secrecy.*

Keywords: *technical surveillance; technical surveillance warrant; interception of phone calls; audio-video surveillance; right to family and private life; postal secrecy.*

Introduction

We are witnessing a profound change of the social environment on a planetary scale. Interpersonal relations are changing, each individual's expectations are growing and the outcome is not always the one expected, thus generating various threats that a few decades ago were unthinkable. We are not wrong to assume that these changes are the most profound in the last few centuries and are generated by the new scientific breakthroughs of the XX and XXI centuries.

It is what we call information technology with explosive growth and huge impact on both social and economic scale. Virtually all parts of our lives are affected by this change, which unfortunately cannot be managed in the current sociopolitical context.

According to specialist, both businesses and most part of social activities are interconnected, existing technologies make machines work with other machines without a human intervention, generating a forth industrial revolution. This revolution consists in the creation of interconnected systems that can gather all sort of information in a world dominated by sensors and devices, as stated by Joe Wilson, CEO in the Microsoft Corporation.

1. Information Technology and citizen safety

From the standpoint of public safety administrators, technology's ability to penetrate our private life makes the concepts of safety or privacy not obsolete or retrograde, but outdated, at least for the time being. Basically anyone can enter an individual's private life using common devices and commit a series of offenses from the comfort of his living room.

The answer to this challenge is not the best, because certain social values and relations adapts harder to reality. Legislative changes are slow, the training of intervention personnel is lengthier, but the most important aspect to take into consideration is the need for safety and therefore solutions must be found.

Discussions regarding the restriction of certain rights and freedoms by law enforcement agencies are not new, but given the current socio-economical and political crisis that affects the globe, these discussions need to bring a new approach on the restriction of certain rights and freedoms of an individual in order to assure the general need for security.

2. The legitimacy and effectiveness of special surveillance methods

The new Criminal Procedure Code introduced an unitary regulation for the use of technical surveillance as means of obtaining evidence in criminal proceedings.

Apart from the ethical aspects that suggest the impact of technical surveillance on private life certain questions arise regarding the legitimacy and effectiveness of such measures.

We agree to the use of technical surveillance for obtaining evidence in criminal proceedings bases on the fact that the technological evolution is used by criminals to prepare and perform criminal acts. In certain cases technical surveillance is the only method to obtain evidence regarding the committal of an offence.

The question is if technical surveillance has been legally used till now and if so, what are the next steps to take for the future use of such means.

In February 2016, the Constitutional Court of Romania issued decision no. 51/2016 which stated that „*in the matter of technical surveillance the only competent authority to use such measures in criminal proceedings is the criminal investigation body and therefore the Romanian Intelligence Service (SRI) is not competent to use technical surveillance in criminal proceedings*". Therefore institutions which are empowered to perform are the Prosecutor or criminal police.

Immediately after the occurrence of the above mentioned decision, Minister of Justice has proposed an emergency ordinance in this regard, which was adopted by the government, namely OUG No. 6/2016. These provisions generated some difficulties among the specialized law enforcement agencies because most of the technical infrastructure was entirely administrated by the Romanian Intelligence Service and another aspect regarded the lack of qualified personnel.

Emergency Ordinance no. 6/2016 stipulated that a certain number of police officer should be detached to DIICOT and DNA, because these agencies have proven in time that use of technical surveillance was efficient. Regarding this aspect, caution is needed when approaching this kind of reorganization. Police officer are part of the criminal investigation body and have been trained in schools of the Ministry of Internal Affairs and even if they are detached to prosecutor offices they are using the Ministry's infrastructure and under no circumstance these officers must not lose contact with the units they came from.

Detaching police officer to prosecutor offices must be made only by the workload and importance of criminal cases under investigation and not by the need of certain prosecutor offices to have more subordinates.

It is known that DIICOT works through delegation some ongoing investigations with police structures from county police departments and this practice is efficient, although police officers from these structures are not remunerated at the same level as specialized structures in fighting organized crime.

3. Some issues regarding technical infrastructure of the judicial bodies

But the biggest problem is the realization of a technical infrastructure that belongs to the judicial bodies, infrastructure that was weak at the time decision No 51/2016 was issued.

At this moment the Ministry of Justice goal is to create such infrastructure available to the prosecutor's office, solution we consider it would not solve the problem but create an even more complicated situation, because technical surveillance is slightly more difficult than it seems:

a. First of all, ***approved and secured equipment must be installed*** at the internet and mobile providers, in accordance to the protocols established between the Ministry of Justice and Ministry of Internal Affairs. This equipment has several characteristics, first of all it must comply with the international standards issued by the European Institute of Standardization Communications, it has to be approved by the Ministry of Justice and not the last the software program must be encrypted and the decryption key must be safely stored in the prosecutor's office. The resulted intercepted communications must be stored on a single memory device and the transcripts of the communications to be made by using the decryption key. This step is very important, because in some cases the defendants contested the authenticity of the intercepted

communications the main reason being that none of the original recordings were encrypted and in theory any person could tamper with these records.

b. Another aspect refers to audio-video surveillance in private spaces, situation when *is needed specialized personnel in unlocking the access doors*. In some cases, the door locks are extremely sophisticated and only highly trained personnel can complete such task. Also surveillance teams are needed in order to choose the best moment for entering a private space and installing the surveillance equipment.

c. Information is needed regarding the suspect, his habits, the particularities of his home and neighbors or persons that may create difficulties in installing the surveillance equipment.

d. At the same time we cannot fail to notice the importance of all data collected in the investigative activities prior to technical supervision with all that this entails, namely intercepting communications, access to a computer system, audio- video surveillance, locating or tracking by technical means and obtaining financial transactions made by an individual or corporation.

The data resulted from technical surveillance must be analyzed and processed by specialized police structures such an Central Unit for Information Analysis and such data resulted must be used in criminal proceedings.

The best solution would be for the Special Operations Unit in the General Police Inspectorate to analyze and process all this data because this unit has access to a wide variety of intelligence, it has specialized surveillance units, interception equipment but only a small number of personnel. The large number of ongoing investigations requires a good systematization coupled with large investments. Creating such units under the coordination of prosecutor offices would create discrepancies in training and remuneration of these specialists, not to mention the investments will be much larger, especially in terms of technical equipment costs.

A solution to this problem would be the creation of a national Center for wiretaps, based on the model used by the Romanian Intelligence Service, but with facilities reported to the volume of ongoing investigations.

The recent reorganization of U.M. 0962 brought an opportunity that should not be overlooked. This will free up a significant number of functions that should be transferred to the Special Operations Division. Please note that these workers have the training and experience to work in this important field. It is possible that some of the equipment owned by the former MAI's Internal Security Unit to be transferred to this unit, thus minimizing the costs and without affecting ongoing investigations.

Basically we think it is necessary that experts specialized in technical surveillance, audio-video surveillance from the former security unit be transferred to the Special Operations Division so technical surveillance activities can continue without syncope.

4. Informing supervised person

Another issue that arouses interest *is informing the surveilled suspect about the being the subject of an technical surveillance measure*. The Criminal Procedure Code stipulates that „*the prosecutor must notify the person in writing within ten days after its termination*". Postponing this notice can be decided by the prosecutor if this would jeopardize other ongoing investigations, if it would jeopardize the victim, the witnesses or their families, or if this would create difficulties in the technical surveillance of other suspects.

In practice, this notice may be missing given the provisions of art. 145 par. 5 of the Criminal Procedure Code which stipulates that the notice can be postponed, but no later than the closing of the investigation. In other words if technical surveillance is used in an investigation and the criminal is not identified and brought to justice, this notice can be issued only when the cases is closed. But if technical surveillance is authorized in a criminal investigation having as object a murder, which is imprescriptibly, the notice can be issued only if the criminal is identified.

The responsibility for this notification rests at the prosecutor offices, but we think that this article should be amended.

It remains to be seen whether this measure is feasible from a practical standpoint because the implications are very large and can generate feelings of irritation and discontent from some people who were intercepted in vain and who think that the recorded material wasn't destroyed or certain intelligence sources may be unmasked. We consider that further research in respect to this matter is needed, especially since there is a real phobia among citizens when talking about wiretaps.

5. Use of data resulting from surveillance in other cases

Another problem is the *use of data resulting from technical surveillance in other cases*. In other words we speak of data obtained from surveillance conducted on a defendant and this data reveals the committal of offences, other than those stipulated in art. 139 par. 2 of the Criminal Procedure Code. According to current regulations, the evidence obtained from the surveillance activities can be used in investigations regarding offenses for which the warrant was issued, but also for other offenses listed exhaustively in art. 139 par. 2 of the Criminal Procedure Code.

However, if results obtained from this surveillance can prove the committal of offenses, other than those specified by the legislature in Article 139 par. 2 of the Criminal Procedure Code, such data cannot be used in other investigations.

We appreciate that this regulation should be changed because of the following arguments: first warrant was issued based on the provisions of the law, then surveillance procedure was strictly followed and last but not least would be a waste of time to repeat the whole authorization process. In support of this proposal we refer to the situation stipulated under Art. 139 par. 3 of the Criminal Procedure Code which stipulates that the recordings made by the parties or other persons can be used as evidence if their object is represented by their conversation or communication with third parties. Otherwise any other recordings can be used, if not prohibited by law.

Conclusions

However, we want to highlight the importance the state must grant to operational structures implementing wiretaps and the importance in providing technical support, logistics and specialized staff carrying such activities.

Last but not least we want to highlight a fact that has important implications in technical surveillance in an online environment. It's about communications conducted via Whatsapp, Viber, Tango, Skype, Facebook, Yahoo Messenger where law enforcement agencies must have the technical capabilities needed to intercept in best conditions such online communications.

But the most important issue is that obtaining such data necessary to carry out an investigation cannot always be achieved due to the opposition of corporations like Yahoo, Microsoft, I.B.M. and so on. In certain cases, these corporations refuse to enforce legal requests made through international law enforcement agencies and based on wiretaps issued by authorized magistrates.

References

1. Convention on the Protection of Human Rights and Freedom, developed by European Council, signed on 04.11.1953 in Rome, enforced at 03.09.1953.
2. Criminal Code and Criminal Procedure Code, Publisher Hamangiu, 2016.
3. Sandra Grădinaru, Technical surveillance in the new Criminal Procedure Code, Publisher C.H. Beck, 2014.
4. PhD Dan Lupaşcu, New Criminal and the New Criminal Procedure Code, Publisher Universul Juridic, Bucharest, 2014.
5. Adrian Petre, Cătălin Grigoraş, Audio and audio-video recordings, Publisher C.H. Beck, Bucharest, 2007.
6. Mihail Udroiu, New Criminal Procedure Code - General part, Publisher C.H. Beck, 2014.
7. Emergency Ordinance no. 6/11.03.2016 for implementing measures on technical surveillance wiretaps in criminal proceedings, published in the Offical Gazette no. 190/14.03.2016.
8. Decision no. 51/16.02.2016 issued by the Constitutional Court of Romania, regarding exception of unconstitutionality of Article 142 paragraph (1) of the Criminal Procedure Code.

= ISSN 2285-0171 ISSN-L=2285-0171