

ASPECTS OF HUMAN RIGHTS INFRINGEMENT BY ABUSIVE USE OF TECHNICAL SURVEILLANCE MEASURES

Petre UNGUREANU
petreungureanu74@yahoo.com

“AL. I. CUZA” POLICE ACADEMY, BUCHAREST, ROMANIA

ABSTRACT

Gathering evidence is a very complex activity carried out by prosecutors during a criminal trial in order to establish the judicial truth. The more complex methods of committing a crime has determined the legislature to react promptly by offering the prosecutors special surveillance methods. One of these methods is the technical surveillance, which according to art. 138 par. 1 consists of the interception of any kind of remote communications, access to a informatics system, audio and video surveillance, tracing or localization by use of technical measures, obtaining the financial records of a person.

Gathering evidence must be carried out by respecting all legal obligations and in accordance with the human rights. This article emphasizes on the infringements on a person's right to private life and secret of correspondence.

Keywords

Technical surveillance, investigative activities, audio-video recordings, expertise on audio-video recordings, informing the investigated person

1. The importance of investigative activities prior to authorizing technical surveillance

Technical surveillance, as stipulated in the Criminal Procedure Code, can be used in obtaining important evidence in a criminal trial. Thus, all investigative activities prior to authorizing technical surveillance must lead to obtaining real and correct data about the committing of a crime.

Art. 139 of the Criminal Procedure Code stipulate as a condition that reasonable data regarding the committal of a crime must be obtained. Art. 140 stipulate that the

request for authorizing technical surveillance made to the rights and freedom judge must contain all evidence and data regarding the committal of a crime. In this context, all evidence and data gathered by the prosecutors must be correct otherwise human rights can be infringed.

For example, when intercepting communications and correspondence over internet applications made by use of a pre-paid SIM, all data obtained by investigative means regarding the person using the pre-paid SIM, the number allocated to the pre-paid SIM must be correct otherwise

infringement to the private life of another person can occur.

“Accidental” interception of another’s person communications and correspondence for obtaining data about the correct phone number of those who are investigated must be avoided.

In Romania, these aspects are topical mostly because communications and correspondence over the internet can be made by use of pre-paid SIMS, without maintaining a database regarding the identity of the persons using such pre-paid SIMS. Thus, the legislature should stipulate the obligation to record the identification data for the users of pre-paid SIMS.

In light of these we propose the drafting of a procedure which contains all investigative measures that have to be executed prior to authorizing technical surveillance by a rights and freedom judge.

2. Aspects of Human Rights Infringement in Transcription of Communications and Correspondence

Art. 143 par. 4 of the Criminal Procedure Code all intercept communications and correspondence with regards to the committal of a crime must be transposed in a report [1].

In practice debates have been carried regarding that transcription the communications and correspondence of a person in a report, without the presence of that person represent an infringement of the right to defense. Art. 92 par. 1 and 143 par. 4 of the Criminal Procedure Code were invoked by giving the right to the defense attorney to assist all acts of criminal prosecution [2].

In our opinion the presence of the defense attorney is not required when technical surveillance is authorized toward a person, who doesn’t have the suspect statute, as prescribed by the Criminal Procedure Code.

In concern to the right of the defense attorney to assist at transcription of the intercepted communications and correspondence art. 92 par. 1 stipulates that the defense attorney cannot assist acts of criminal prosecution that concern technical surveillance measures. Also the right to defense must be

taken in consideration and this implies that all communications and correspondence must be transposed in a report in a manner that is not susceptible to change the general meaning of the words and context by using the exact words of the persons involved. The report must be then certified by the prosecutor, as a guarantee that the report generated contains the exact state of fact as the one resulted from the communications and correspondence. The report must not contain the communications and correspondence which are relevant to the cause.

In some cases, the report does not contain communications or correspondence regarding other persons or crimes, other than the ones stipulated in the technical surveillance warrant, assuring in this way the confidentiality of criminal prosecution with regards to other crimes that are under investigation.

The transcription of communications and correspondence is made by specialized police officers or by agents of other services generally materialized in notes that are given to the prosecutor and the report is generated based on these notes. In this matter we suggest that the specialized police officers and agents (for example Direction of Special Operations) receive the possibility to transpose and generate the report that can be used as evidence in a criminal trial. This measure should apply for agents of other services too, by allowing generating of notes, prior to the report. In all cases the prosecutor must personally transpose audio-video communications intercepted by technical surveillance.

3. Usage of reports generated by technical surveillance methods in other criminal proceedings

The Criminal Procedure Code stipulated that data or information obtained through technical surveillance can be used in other criminal proceedings if such data or information is concluding and regards preparation or committal of other crimes.

European Court for Human Rights stipulated that intercepting a communications

made by the defendant with another person, subject to technical surveillance and usage of those communications is an infringement of privacy, as stipulated in art. 8 of the Convention [3].

An issue regarding human rights is the possibility given to prosecutors to evaluate the data and information obtained by technical surveillance that is not conclusive and is not relevant for use in other criminal proceedings. The Criminal Procedure Code does not contain a control mechanism regarding the evaluations made by the prosecutor and therefore a possibility exists that certain data and information are deemed irrelevant, although are relevant to the case or other criminal proceedings.

In order for such data and information be used in other cases or criminal proceedings, the legislature should enforce the rights and freedom judge that issued the technical surveillance warrant to be able to issue a new warrant for the new crimes that are discovered. Otherwise the warrant could be deemed illegal.

4. Usage of Recordings Made by the Parties in Criminal Proceedings

The Criminal Procedure Code stipulates that recordings made by parties can be used as evidence in criminal proceedings if they contain communications or correspondence in which the parties participated. These recordings are considered to be obtained outside criminal proceedings, but can be used as evidence if they are not contrary to the law.

In practice, the victim/witnesses/other persons request that the prosecutors provide them with the technical means of intercepting and audio-video recording communications or correspondence they have with other parties. In such cases if the prosecutor uses the recordings, judicial practice considered such recordings illegal.

Recordings made by parties can be used in criminal proceedings as evidence or can be used in front of a rights and freedom judge to obtain a technical surveillance warrant.

The Supreme Court of Romania stipulated that recordings obtained by parties, using technical means of intercepting and audio-video recording communications or correspondence provided by the prosecutors are illegal [4].

European Court for Human Rights also considered that recordings made by parties using technical means of intercepting and recording provided by prosecutors are illegal and represent an infringement of the right to privacy and private life as stipulated in Convention of Human Rights art. 8.

The problem that poses a great interest is whether the records made by video surveillance systems installed by individuals can be used in criminal proceedings when concerning the public domain.

European Court for Human Rights considered a violation of privacy and private life the use of video surveillance systems in a manner that focuses on a certain person (redirecting or repositioning the systems, installing components in specific areas etc.) [5].

Authorities in such cases must not offer “assistance” to the operators in installing video surveillance systems or components of those systems in specific areas or aimed at a certain person.

Another violation of the right to privacy and private life consists of divulgence to the mass media of images/ transcripts regarding the person under investigation [6].

5. Expertise of Audio-Video Recordings and Photos

In practice, in many cases the person under investigation contested the authenticity of audio-video recordings or photos obtained during a criminal trial by use of technical surveillance. Regarding transcripts of audio recordings both the content and meaning of text was contested. The contested recordings are analyzed by the National Institute of Forensics, institution coordinated by the Ministry of Justice. In the literature great importance has been given to analyzing and expertise on authentic recordings as a condition for usage of these recordings as evidence [7]. Based on the analysis and

expertise techniques the specialists can provide information about audio-video recordings or photos regarding date and time of creation, existence of deletions of the content and the durations of these deletions, if the recording was initially generated using the digital compression capabilities of the equipment provided [8].

The difference between original recordings and copies is hard to distinguish. Even the Criminal Procedure Code refers in art. 143 par. 2 to storage of the original media or the certified copy sealed in special spaces in the Parquets and at disposal of the court if needed. The Code also refers to the possibility of certifying the copies by using an electronic signature.

The issues the parties are addressing concern the lack of certain fragments of the recordings or voice recognition. In the scientific community there is no minimal standard regarding voice analysis [9]. Also, given today's technological capabilities alteration of such recordings is possible by erasing, adding or intercalation of words/ phrases).

In order to enforce protection the rights to private life and privacy we consider that the prosecutor, by default should expertise audio-video recordings, especially in cases where most of the evidence is based on such recordings. Expertise should be made based on art.172 Criminal procedure Code and if alteration of these recordings is observed the recordings should be removed as evidence, in accordance to the Criminal Procedure Code, art. 102 par. 2.

6. Notifying investigated person

The new Criminal Procedure Code stipulated that the person who was investigated by technical surveillance methods is to be informed about this measure in maximum 10 days after the termination of the warrant. The person is granted access to the transcripts that resulted from the use of technical surveillance and, on demand, can hear or watch the audio/video recordings. The person interested must file a request at prosecutor's office in 20 days after receiving the notice.

In certain cases, the prosecutor can postpone this notice or provide audio/video recordings if this is necessary for the pending investigation or it would represent a threat to the safety of the victim's, witnesses' or family members or if it would jeopardize technical surveillance of other persons. In these cases the notice can be postponed no later than the closing of the investigation [10]. These measures are in accordance to the judicial practice of the European Court for Human Rights [11].

In practice some difficulties appear in cases where technical surveillance measures are used regarding certain persons, cases in which prosecution is made without toward the crime, without having a suspect or a defendant. In such cases the notice is postponed by the prosecutor, in accordance with art. 145 al. 4 Criminal Procedure Code until a solution is given in the case. In accordance with the Convention for Human Rights we consider that a maximum limit of time for which the prosecutor can postpone the notice must be enforced so that the notice cannot be postponed until the criminal liability prescription occurs.

7. Conclusions

In our opinion, the use of technical surveillance in judicial proceedings can lead to infringements of an individual's human rights. This infringement can occur during the preliminary investigations, prior to the authorization for use of technical surveillance but also during the use of such means. An important aspect that can generate infringement of an individual's human rights regards the moment when the investigated person must be notified about the use of technical surveillance, but also when data or information obtained by use of technical surveillance can be relevant in other judicial proceedings.

Use of technical surveillance, in terms of protecting an individual's human rights must not generate problems in ongoing judicial investigations. A very important aspect is given by the fact that new methods of committing criminal acts have evolved and the latest technology can be used in

committal of crimes, generating problems in discovering and investigating crimes.

In this context, use of technical surveillance is justified, but on the other hand an efficient control mechanism must be created that can guarantee the use of technical surveillance only in legitimate ways.

In conclusion, a balance must be preserved between the use of technical

surveillance in investigations regarding criminal acts and national security and protecting an individual's private life in accordance with the legal provisions of a democratic society. This balance can only be preserved by a human rights judge who is the only authority who can authorize or infirm the use of technical surveillance.

References

1. Conf.univ.dr. Dan Lupașcu, *New Criminal Code and the New Criminal Procedure Code*, (Bucharest: Universul Juridic Publishing House, 2014), art. 143 al. 4.
2. Sandra Grădinaru, *Technical Surveillance methods in the new Criminal Procedure Code* (Bucharest: C.H.Beck Publishing House): 282.
3. European Court for Human Rights, *Kruslin vs. France* 24.04.1990
4. Supreme Justice Court of Romania, *Criminal sentence nr 4286/18.09.2007*
5. European Court for Human Rights, *Amann vs. Switzerland* 16.02.2000
6. Prof.univ.dr. Dumitru Virgil Diaconu, *Pătrunderea în spații private în cazul tehnicilor speciale de supraveghere sau cercetare*
7. Adrian Petre, Cătălin Grigoraș, *Înregistrările audio și audio –video*, (Bucharest: C.H.Beck Publishing House): 201.
8. B. Koenig, D. Lacey, *Applications of ENFAnalysis in Forensic Authentication of Digital Audio and Video Recordings*, *J.Audio Eng. Soc. Vol 57, No. 9, September 2009*, citat de Adrian Petre, Cătălin Grigoraș în *Înregistrările audio și audio –video*, (Bucharest: C.H.Beck Publishing House): 202
9. Adrian Petre, Cătălin Grigoraș, *cit.ed.*, p. 212
10. Conf.univ.dr. Dan Lupașcu, *cit.ed.*, art. 145 al. 5
11. European Court for Human Rights, *Klass vs. Germany* 06.09.1978

Acknowledgement

This work was possible with the financial support of the Sectoral Operational Programme for Human Resources Development 2007-2013, co-financed by the European Social Fund, under the project number **POSDRU/159/1.5/S/138822** with the title “*Transnational network of integrated management of intelligent doctoral and postdoctoral research in the fields of Military Science, Security and Intelligence, Public order and National Security – Continuous formation programme for elite researchers – «SmartSPODAS»*”.

Bibliography

- Prof.univ.dr. Diaconu, Dumitru Virgil. *Pătrunderea în spații private în cazul tehnicilor speciale de supraveghere sau cercetare*.
- Grădinaru, Sandra. *Supravegherea tehnică în Noul Cod de Procedură Penală*. Bucharest: C.H.Beck Publishing House.
- Conf.univ.dr. Lupașcu Dan, *Noul Cod Penal și Noul Cod de Procedură Penală*. Bucharest: Universul Juridic, 2014.
- Petre, Adrian, Cătălin Grigoraș. *Înregistrările audio și audio – video*. Bucharest: C.H.Beck Publishing House, 2007.