Eximia Journal

(ISSN 2784-0735)

Vol. 12

2023

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Surveillance methods

Rotaru Bianca Stefania

Independent researcher

Abstract. Considering that with the passage of time the manner of committing crimes, in many cases, poses serious problems regarding the possibility of probation, it was necessary to register changes in the matter of evidence in order to improve the technical possibilities of administration. Thus, by Law no. 141/1996, the Audio or Video Recordings section was introduced, widening the scope of evidence to include audio recordings and video or photo image recordings. Shortly after, namely in 2003, by Law no. 281/2003, the possibility of administering such evidence was expanded, the title of the section being Interceptions and audio or video recordings. The seat of the matter regarding evidentiary procedures: interception and recording of conversations or communications, audio-video recordings, filming is constituted by art. 91 ^{1}-91 ^{6}. In addition to these procedural provisions, there are also special laws that provide for access to telecommunications or IT systems as means of evidence, such as: Law no. 143/2000 on combating drug trafficking and illicit drug consumption, which provides in art. 23 that the criminal investigation body with the authorization provided by law can have access for a determined period to the telecommunications or computer systems and supervise them with the appropriate application of art. 91 ^{1} -91 ^{6} Criminal Procedure Code; Law no. 678/2001 on preventing and combating human trafficking and Law no. 656/2002 on the prevention and sanctioning of money laundering with similar provisions on access to telecommunications or IT systems; Law no. 78/2002 regarding the fight against corruption and Law no. 161/2003 regarding some measures to ensure transparency in the exercise of public dignities and the sanctioning of corruption shows that there is the possibility of surveillance or interception of communications, access to information systems for all types of communications, regardless of whether they are carried out through telephone lines or in another way.

Keywords. Notices, police intervention, restoration of order, individual resources, legality

I. General Considerations Regarding Audio/Video Interceptions and Recordings

I.1. The notion and legal framework of interceptions

As a result of the inviolability of correspondence and telephone conversations, enshrined as a fundamental citizen's right in democratic constitutions, initially it was not allowed to use the recording of a conversation or communication in court, as an action of the courts. The amplification of the criminal phenomenon, through the use of technical means of communication, determined the acceptance, under certain conditions, of the use of interceptions and recordings of telephone conversations and other communications, especially in the case of those crimes whose probation was not otherwise possible.

The possibility of audio-video interception and recording by state authorities is provided for in most legislation, being linked, in most cases, to the fight against organized or ordinary crime, the internal legislative framework being assessed according to compliance with the

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

provisions of art. 8 of the European Convention on Human Rights, which guarantees everyone the right to respect for his private and family life, his home and his correspondence. In the opinion of the European Court of Human Rights, there is correspondence in all situations where two or more people exchange, in any way, on any medium, a message or an idea. The notion of communication includes written, telephone or radio-telephone communication, as well as that by electronic means.

In principle, a regulation corresponds to the provisions of the Convention if, whatever the system of interception and recording, there is a system of adequate and sufficient guarantees against possible abuses. Of course, such assessment has a relative character, depending on the circumstances of the case, such as the duration of these measures, the reasons for which they were ordered, the execution and control of their execution, the possibility of contestation, as well as their effects. Only if solid guarantees against the abusive use of these means of evidence can be found, the risk of interference with the right to correspondence can be eliminated. For example, "interception of telephone conversations" [1]is a serious interference in a person's private life and correspondence, which is why it must be based on a legal basis that includes a certain degree of precision in regulation. It is essential to have clear and detailed regulations in this field, precisely to eliminate abuses.

In our country, Law no. 51/1991 regarding national security (art. 13) provided for the possibility of interception and recording of telephone conversations and other communications in case of preparation and commission of crimes that are threats to national security; then, Law no. 26/1994 on the Romanian Police extended this possibility also in the case of organized crime and serious crimes, if it was necessary to carry out the criminal investigation. By Law no. 141/1996 for the amendment and completion of the Criminal Procedure Code, a new Section was introduced into the Code, *with art.* 91 [1] -91 [6] , under the name " *audio or video* recordings", after, by art. 64, audio or video recordings and photographs were added to the means of evidence. Finally, after a period of application of the new provisions, through Laws No. 281/2003 and 356/2006, new regulations were introduced: Section V [1] acquired a broader name "Interceptions and audio or video recordings", limiting their scope of action and strengthening- the legal framework in which they can be used.

Audio-video recordings are listed in art. 64, as means of evidence, while wiretapping is the process by which recordings are obtained as means of evidence. The doctrine qualified the audio-video interceptions after the time of their execution, as evidentiary procedures, if they are carried out after the start of the criminal investigation, respectively preliminary documents, if they are carried out before the start of the criminal investigation. [2]Audio or video recordings, as means of evidence, are those magnetic tape recordings of conversations and image recordings whose content results in facts or circumstances of a nature to contribute to finding out the truth.

"Interceptions" - the intervention of authorized bodies in any kind of telephone conversations or communications or through any electronic means of communication - radio, private and indoor television, not subject to publicity - which implies the idea of confidentiality between those who carry it out. Audio recordings include prints on magnetic tape or on any other medium of conversations or communications, whether they are intercepted authorized or to be made in the future, at a certain time and in a certain place, between two or more people; they consider microphones placed in certain rooms, in certain places, to record conversations or communications, without the people performing them knowing that they are being recorded.

[1] Ivan Anane, *The Investigation and tracking of criminals*, Pro Universitaria Publishing House, Bucharest, 2014
[2] Dorel L. Julean, *Criminal procedural law – general part* , West University Publishing House, Timișoara, 2010

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

The law also refers to video recordings - of images that include operative photos and films, executed by criminal investigation bodies without approval or without the knowledge of those recorded. The image recordings also include the recordings made by means of equipment hidden from view, in banks, institutions, large stores, through which the persons who enter, act and leave the places where the recordings are made are recorded, constituting means of identification of the persons who possibly prepare or commit crimes. Under the terms of the law, recordings can be made in the ambient environment, locations or tracking by GPS or by other electronic means of surveillance. Finally, audio or video recordings can be made by persons who are or may become parties to a criminal case, through their own audio or video equipment. The importance of the regulation of wiretapping derives from the fact that the constitutional principle of the protection of intimate, family and private life (art. 26 of the Constitution) or of the secrecy of correspondence (art. 28 of the Constitution) is inviolable, with the limitations imposed by the necessity of criminal investigation (art. 53 of the Constitution). From the perspective of ECtHR jurisprudence, interception and audio-video recordings represent an interference by public authorities in the right to private life and correspondence. Such an intervention will violate art. 8 of the European Convention, if it does not comply with the legal provisions, it does not have one of the purposes provided by art. 8 and is not necessary in a democratic society to achieve this goal.[3]

I.2. Interception procedure

The authorization procedure for interceptions and recordings of conversations or communications has the following stages:

- the proposal of the prosecutor who carries out or supervises the criminal investigation. The proposal can be made ex officio, at the request of the criminal investigation body or at the request of the injured person;
- the resolution competence belongs to the president of the court that would have the competence to judge the case in the first instance or from the corresponding court in whose district the office of the prosecutor's office is located, of which the prosecutor who carries out or supervises the criminal investigation is a part. In the absence of the president, the authorization is made by the judge appointed by him. The procedure takes place in the council chamber;

The act authorizing the interception and recording of conversations or communications is the conclusion of the meeting, which will include:

- the concrete indications and facts that justify the measure;
- the reasons why the establishment of the factual situation or the identification or location of the participants cannot be done by other means or the research would be much delayed;
- the person, means of communication or place subject to surveillance;
- the period for which interception and recording are authorized. [4]

In this way, the conditions are created for a control over the authorizations given, with regard to the crimes for which the measure was ordered, the information that justifies it, the authorized time duration, control to prevent any abuse.[5]

[3] Dorel L. Julean, *Criminal procedural law – general part* , Western University Publishing House, Timisoara, 2010
[4] Nicu Jidovu, *Criminal Procedural Law , 2nd Edition* , CH Beck Publishing House, Bucharest, 2007
[5] Grigore Gr. Theodoru, *Treatise on Criminal Procedural Law, 2nd Edition*, Hamangiu Publishing House, Bucharest, 2008

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Authorization is given for the duration necessary for interception and recording, but not for more than 30 days. The authorization can be renewed; before him after the expiration of the previous one, under the same conditions, for thoroughly justified reasons, each extension not exceeding 30 days. The total duration of authorized interceptions and recordings, regarding the same person and the same deed, cannot exceed 120 days.

The question arises whether authorization for interception and audio or video recording can be given only after the start of the criminal investigation or and before this, as a preliminary act of *criminal* prosecution . It was shown that by Law no. 281/2003 added art. 100, in the sense that the search cannot be ordered before the start of the criminal investigation, which was not provided for "interceptions and audio or video recordings" [6], although the texts regarding these means of evidence were also modified. Since audio or video recordings can be authorized when they are given and about the preparation for the commission of serious crimes and for the identification or location of criminals, which also involves information work, in the absence of a prohibitive text, these recordings can also be made as a preliminary act , if authorized by law. The prosecutor is obliged to order the immediate cessation of audio or video interception and recording, even before the expiration of the authorization period, if the reasons that justified them no longer exist, informing about this court that issued the authorization.[7]

I.3. Certification and probative value of interceptions

Law no. 356/2006 expressly repealed the procedure of verification by the judge of the legality and usefulness of interceptions and recordings of conversations and communications. However, this procedure represents the first direct application of art. 64 para. 2 and thus constitutes a procedure for verifying the validity of the evidence, a procedure carried out before the court is referred to the merits of the case. The previous form of art. 91 [3] represented an unprecedented procedure for the Romanian system, but at the same time completely natural considering the provisions of art. 64 para. This idea had to be followed by Law no. 356/2006, and to ensure the effectiveness of art. 64 para. 2 the procedure had to be extended to all means of evidence in the form of a preliminary procedure on the merits. In diametrically opposite sense however , without a real justification, Law no. 356/2006 repealed it.

Thus, art. 91 [3] C.proc.pen. provides that the report of the rendering in written form is certified for authenticity by the prosecutor who carries out or supervises the criminal investigation in question. Correspondence in a language other than Romanian is transcribed into Romanian by means of an interpreter.

When presenting the criminal investigation material, the prosecutor is obliged to present to the accused or defendant the minutes in which the recorded conversations are reproduced and to ensure, upon request, their listening, precisely as a guarantee of the exercise of the right to defense.

If in the case a non-trial solution was ordered, the prosecutor is obliged to inform about this person whose conversations or communications were intercepted and recorded. The support on which the recorded conversations are printed, they are archived at the prosecutor's office, in special places, in a sealed envelope, with the assurance of confidentiality, and they are kept until the expiration of the statute of limitations for the criminal liability for the deed that formed the subject of the case, when they are destroyed, ending the process- verbally to this effect.

[6] Gheorghe Buzescu, *Theory Rules and practice for police usage*, Pro Universitaria Publishing House, Bucharest, 2016

[7] Grigore Gr. Theodoru, *Treatise on Criminal Procedural Law, 2nd Edition*, Hamangiu Publishing House, Bucharest, 2008

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

In case *of resumption of criminal investigations*[8] in that case or for other crimes, the support can be consulted or copied only by the prosecutor who carries out or supervises the criminal investigation.

The insertion of the provision from art. 91 para. (6) the final thesis that, in the other cases, these activities of consulting or copying the records could take place only with the authorization of the judge is difficult to implement, as he does not have the practical possibility to be aware of the entire interception activity carried out by competent authorities.[9]

After archiving, the medium on which the recorded conversations are printed can be consulted or copied in the case of the resumption of investigations or under the conditions provided for in art. 91 [2] para. (5) C. proc. pen and only by the prosecutor who carries out or supervises the criminal investigation, and in the other cases only with the authorization of the judge

If in the case the court pronounced a judgment of conviction, acquittal or termination of the criminal process, which remained final, the original support and its copy are archived together with the case file at the court's headquarters, in special places, in a sealed envelope, with the assurance of confidentiality. After archiving, the medium on which the recorded conversations are printed can be consulted or copied only under the conditions stipulated in art. 91 [2] para. (5), with the prior approval of the president of the court.

A special situation arises when crimes are committed through conversations or communications containing state secrets. In such circumstances, the criminal procedural law provides that it is necessary to draw up separate minutes in which to mention the conversations or communications or their passages that constitute state secrets, the certification being carried out according to the common procedure.

Consistent with the principle of free evaluation of evidence, the Romanian legislator did not privilege (in the new regulation) the probative power of audio or video recordings. In this sense, art. 91 [1] orders that these records they can serve as means of proof if their content results in facts or circumstances likely to contribute to finding out the truth. The rule of corroborating the means of proof in carrying out the activity of their appreciation remains valid in this hypothesis as well.

In art. 64, audio or video recordings are entered as evidence. In reality, these are evidentiary procedures, because they consist of a series of technical operations, recording and transcription, carried out by technicians, with appropriate certifications, which are finalized in a report, which has become the means of evidence in which the conversations and communications or in which there are images, which are evidence.

Being passed among the means of proof, it is written as a general rule that the evidence has no predetermined value, which means that they can contribute to finding out the truth to the extent that they form the confidence that they correctly reflect the existence and content of some conversations or the image of some people, objects, places. Undoubtedly, for those who have the obligation to evaluate the evidence, these interceptions and recordings give them confidence, because they were obtained without the knowledge of those who were audio or video recorded and to hide real facts or to invent unreal facts.

[8] Gheorghe Buzescu, *The place and role of the civil servant in the state apparatus*, Sitech Publishing House, Craiova, 2017
[9] Nicu Jidovu, *Criminal Procedural Law*, 2nd Edition, CH Beck Publishing House, Bucharest, 2007

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

It is known, however, that the technique today allows some recordings to be falsified, either by taking over only parts of the conversations or communications that took place in the past and declared as recently recorded, by removing from the text some parts of the conversations or communications , either by transposing or removing some images. It is the right of those interested - the parties to the trial, the prosecutor, the court - to have doubts about the correctness of what is recorded, in whole or in part, especially if it does not fit into the set of evidence administered. In case of such suspicions of falsification, at the request of the prosecutor, the parties or ex officio, the court may order the submission of the audio or video recordings to technical expertise, which will verify the authenticity and continuity of the recordings.[10]

As a result, these audio or video recordings serve as evidence in the criminal process by themselves, if they are not contested, or by their confirmation by technical expertise, if there were doubts about their conformity with reality. If the technical expertise finds the lack of authenticity of the recordings or the intervention in the text through mixes or removal of passages from conversations or through image tricks, the audio or video recordings cannot be retained in the settlement of the case; based on art. 64 para. (2) they cannot be used as evidence in the criminal process when they were made in violation of the legal provisions. According to art. 91 [1] para. (6), the recording of the conversations between the lawyer and the party he represents or assists in the process cannot be used as a means of evidence unless it contains conclusive and useful data or information regarding the preparation or commission of a crime by the lawyer , among those provided by law as a condition for authorization of interception [11].

Audio or video recordings presented by the parties may serve as evidence; these recordings may be made by amateurs or professionals, before or during the trial; they can serve as evidence when looking at their own conversations or communications they have had with third parties. Any other recordings may constitute evidence if they are not prohibited by law, such as those regarding a person's private life for the purpose of blackmail, pornography, etc.

II. Technical means and recording

II.1. Interception and recording of conversations

Communications can be recorded in two ways: with the knowledge of one of the people communicating, controlling the means of communication used by them, or without the knowledge of any of the people involved through interception activity.

In the first case, the recording of telephone communications made from stations in fixed or mobile telephone networks can be carried out by:

a) connecting a technical means to the circuit of the fixed telephone station that is supervised or to another additional circuit, which is added to the primary one;

b) connecting to the mobile phone a device (hands-free type) [12]that ensures the reception and transmission of the audio signal to the recording device;

c) placing the microphone of the recording device near the speaker of the micro-receiver of the classic telephone or the speaker of the mobile phone, so that the respective

[10] Grigore Gr. Theodoru, *Treatise on criminal procedural law,* 2nd Edition, Hamangiu Publishing House, Bucharest, 2008

[11] *Art. 33 para. (2) from Law no. 51/1995* on the organization and exercise of the profession of lawyer, the telephone conversations of the lawyer cannot be listened to and recorded by any technical means, nor can his professional correspondence be intercepted, except under the conditions and with the procedure provided by law

[12] Gheorghe Buzescu, *The place and role of the civil servant in the state apparatus*, Sitech Publishing House, Craiova, 2017

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

microphone records both the sounds from the ambient environment (the voice of the person using the device) and those transmitted through the telephone network (the voice of the interlocutor).

In the second case, when telephone communications are intercepted and recorded without the knowledge of the people communicating, these operations are currently carried out through the National Communications Interception Center (CNIC), administered by the Romanian Intelligence Service. The system has national coverage and ensures, under the law, the taking over of the traffic of any agent qualified to operate a network or provide authorized telecommunications services. Also, the system is fully computerized and is configured in such a way that it works automatically, excludes and signals any unauthorized intervention, including from the operators who serve it.

GSM» (Global System for Mobile Communications) [13]is a European mobile communications system created in 1986 as a military application and which has been used commercially, in a unified way, since 1991.

Each GSM terminal and each SIM card with which it is equipped have a unique code: the IMEI code (International Mobile Equipment Identity) corresponding to the phone and the IMSI code (International Mobile Subscriber Identity) for the phone card.

This pair of codes defines, at a given moment, any user of GSM services, and their knowledge is essential for the individualization of the GSM device, the identification of the respective person and the area in which he is located, as well as for the interception and recording of telephone communications made through GSM terminals .

In principle, the interception of telephone communications using the mentioned national system is carried out through the connections between the system and the switchboards of the telephone exchanges of the fixed telephone networks and, respectively, the switching centers of the GSM telephone networks. When the situation requires it, telephone communications can be monitored in real time (the so-called recording), the system operators immediately informing the criminal investigation bodies about the content of all conversations that take place through the monitored telephone set.

As is known, there are three large GSM operators in Romania: Connex — Vodafone and Orange have a license on 900 Mhz, and Cosmote has a license on 1800 Mhz (also called DCS). To densify the network, Vodafone and Orange also use the 1800 Mhz band in the big cities, and Cosmote also installs EGSM (900 Mhz) to increase its coverage outside the cities and even inside the cities to improve it (in basements, for example). Vodafone also launched a UMTS network, and Zapp operates a CDMA network.

900 Mhz has the advantage of propagating further and penetrating obstacles better (concrete walls, for example); his problem is that only 124 channels are available, 63 for each operator in Romania, which is far too few at the moment to avoid the situation of Network Busy in cities.

The 1800 Mhz operates less far than the 900 and penetrates obstacles more difficult. The advantage of 1800 is that in total there are 374 channels available (3 times more than in GSM), so it is installed specifically to densify the network where the addition of new 900 Mhz BTSs is no longer possible (because of the frequency reuse reason).EGSM still uses the 900 Mhz band, only it emits a little higher for the up-link and a little lower for the down-link than the basic 900 Mhz (because of this, not all phones are EGSM compatible).

[13] Gheorghe Buzescu, *Peculiarities of contraventional law*, Sitech Publishing House, Craiova, 2017

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

UMTS, which is also called 3G or WCDMA (because it is based on CDMA technology, like Zapp), emits in 2100 Mhz. In this frequency, the coverage is very small (for example, in 1800 Mhz you can reach up to 30 km, but in UMTS more than 10 km is not exceeded in open ground).

In addition to the advantage of tracking the target from its proximity and that of total confidentiality, the use of such special equipment is prohibitive, due to the very high costs of acquisition and the highly qualified personnel required to service them. Such radio reception equipment, based on scanning or monitoring the radio frequency spectrum, can also be used to intercept and record radio communications. The clarifications made previously are also valid as regards the interception of other types of communications, such as those carried out by fax, cordless phones, messages written via GSM networks (SMS), via the Internet (e-mail) [14]or others. For fixed networks there are also and the solution of connecting devices to be recorded on the telephone circuits, at different points of the telephone cables or on additional telephone circuits, connected for this purpose over the targeted telephone circuit.

This method and others of this kind are not used, as they present major risks of uncovering conspiracies, unacceptable in the conditions of the existence and operation of the national system of interception of telephone communications. In order to implement the authorizations issued under the law, the competent bodies and the persons who give technical contest proceeds, during the authorization period, to the continuous interception and recording of telephone communications or other types of communications or to the sporadic recording (especially in the case of ambient conversations), when operative moments arise, which necessarily implies keeping under permanent observation of the targeted persons (called "targets", "vectors" or objectives in the informative-operational activity).

II.2. Realization of interception in the ambient environment

In order to carry out interception and recording operations, it is necessary that judicial police officers and technicians be provided with minimum data, which often exceed the data mentioned in the authorization documents.

Such data allow the correct choice of concrete action methods and technical means and may refer to the criminal activity, the personality of the perpetrators, the methods used by them, the place and time of the meetings to be monitored, etc.

The selection of the type and performances of the special technical means to be used is made according to the following general requirements:

- ✓ the purpose for which they are used;
- ✓ the need for camouflage and concealment;
- ✓ the environmental conditions and other conditions in which the registration is carried out;
- ✓ the characteristics and technical parameters, especially the way of storing the information and the autonomy of operation, given by the storage capacity and the viability of the power source.

In order to understand the nature, mode of operation and performance of various types of technical means, some clarifications are necessary for each of them.

From the point of view of their type, it is preferable to use audio-video recording means that ensure the retrieval of a maximum volume of information from the monitored environment and present the advantage of temporal synchronization of sounds and images.

[14] Gheorghe Buzescu, *The place and role of the civil servant in the state apparatus*, Sitech Publishing House, Craiova, 2017

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Cable transmission to storage media has the advantage that it does not require further operations and the said media have a high degree of maneuverability, while recording on embedded media has the advantage of greater storage capacity and recording continuity.

The performance means of digital recording, audio and video) ensure a very high quality of the obtained results, and if the recording is done on the principle of static memory, the download of the obtained information can be done almost instantly through a USB interface with a high transfer rate, directly on the personal computer, with all the advantages that arise as far as the possibilities of storing and processing information are concerned.

The technical means of recording with radio broadcast transmission consist of recording sets consisting of a microphone (sometimes also a video camera) [15]and a modulated transmitter, which receives and transforms sound and images, which it transmits in the form of radio signals to a receiver and a recording device, which transform radio waves into electrical signals and, respectively, store the information obtained on a magnetic or any other type of support.

The complete interception and recording can be completed by means of a repeater type radio relay which, placed within the range of the transmitter, receives and amplifies the signal emitted by it, after which it retransmits them to the receiver, which can be located at considerably greater distances.

The choice of transmitters is made according to the distance from which the reception is carried out (this being directly proportional to the power of the respective transmitter), the characteristics of the environment (the existing obstacles), the duration of operation (the power being inversely proportional to the operation time), etc. The main vulnerabilities of such equipment consist in the quality of reception, limited range of action and the possibility of interception of the transmission by unauthorized persons (if the information is not encrypted). Another restrictive element is the operating time of the power source, but this shortcoming can be overcome by using remote-controlled transmitters, which can be turned on and off remotely, thus ensuring the possibility of longer operation.

The essential advantage of using such technical means consists in the possibility of real-time reception of transmitted sounds and images, which is why such means are used during actions that require, at a given moment, the intervention of the operative team, especially in the case of detection of crimes blatant. On the other hand, the means with local transmission do not allow a real-time monitoring of the recorded information, but present, under any conditions, a guarantee of the quality and continuity of the recording.

Simply speaking, these evidentiary procedures involve three major operations:

1) installation (mounting, placing, fixing);
2) maintenance (maintenance in operation by changing or charging power sources, by replacing information storage media or by repairing defective components);
3) the recovery (lifting) [16]of the technical means of interception and recording.

Considering the degree of miniaturization achieved in the construction of such components, their masking is possible in a wide range of objects, ranging from concealment in clothing, furniture elements, electrical or electronic items, personal items to their placement in the existing building elements in the spaces of interest.

[15] Ivan Anane, *Elements of Theory and Tactics of the Pursuing of Criminals*, Pro Universitaria Publishing House, 2014
[16] Gheorghe Buzescu, *Police law - university course*, Sitech Publishing House, Craiova, 2019

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Practically, the only possible limits in this field are those set by the imagination and experience of judicial police officers, technicians and specialists.

Each activity of interception and recording of conversations or communications has a unique and unrepeatable character, presupposing technical or procedural risks, as well as the assumption, to the highest degree, of the responsibility of those who perform it. At the same time, this is not a mechanical or isolated activity, in the sense that it involves a complex of previous activities, aimed at the procedural and technical preparation of the records and fixing precisely the moment of their performance. Also, each interception and/or recording activity, an activity that has a certain degree of complexity in itself, is preceded by a detailed technical study, which has the role of establishing the concrete conditions in which the registration will be made, including the categories of technical means that will be used.

Often, in practice, obtaining a proper recording lasting only a few minutes requires days of work on the part of the investigation team, technical innovations and spontaneous reactions to incidents that may arise during the course of actions.

II.3. GPS location and tracking

In the technical literature, the acronym GPS derives from the English name Global Positioning System, which refers to the network of geostationary satellites that, through the transmitted data, allow the geographic positioning of a receiver. Originally invented as a military application, GPS tracking or tracking permanently records and transmits the activity of a vehicle or other carrier 24 hours a day, regardless of whether it is stationary or moving. The location information is obtained from the satellites of the GPS system and is transmitted between the mobile equipment mounted in the vehicle and the central server of the system using, in some cases, GPRS type services. Some equipment allows the route to be stored in the internal memory of the mobile unit, ensuring the possibility of their retransmission in case of link failure (see, for example, a complete GPS module) [17].

Using the goniometry system, it is possible to determine the direction from which a certain GSM phone emits or its location, even if the GSM phone is in stand-by mode. Normally a switched on mobile phone rarely emits signals, except when engaged in a conversation. For this reason, systems of this kind cause the mobile phone to emit a signal (the so-called hidden call), without the user realizing this. The system informs the ranging unit about the start and end of this hidden call and also about the IMSI and IMEI of the mobile in question.

III. Supervision and investigation through the Criminal Procedure Code project

III.1. Special surveillance and interception techniques

In the vision of the Project of the New Criminal Procedure Code, the interception of conversations and communications, video, audio or photography surveillance in private spaces or location or tracking by GPS or by. other technical means of surveillance are included in Chapter II, suggestively named Technical means and recording. The marginal name of art. 136 - General provisions - provides indications regarding the regulatory modality, completely different from the Criminal Procedure Code in force. Thus, paragraph (1) of art. 136 exhaustively lists the specific methods, namely:

a) interception of conversations and communications;
b) video, audio or photography surveillance in private spaces;
c) locating or tracking by GPS or other technical means of surveillance;
d) obtaining the list of telephone conversations;
e) detaining, surrendering or searching postal items;

[17] Gheorghe Buzescu, *Elements of public order*, Pro Universitaria Publishing House, Bucharest, 2016

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

f) monitoring of financial transactions and disclosure of financial data;
g) the use of undercover investigators;
h) detection of a corruption offense or the conclusion of an agreement;
i) supervised delivery;
j) identifying the subscriber, owner or user of a telecommunications system or a computer access point.

Starting with paragraph (2) of art. 136 the drafters of the Project understood to define each tactical procedure, showing that interception of conversations or communications is understood as interception; access, monitoring, collection or recording of conversations or communications made by telephone, computer system or any other means of communication, as well as the recording of traffic data indicating the source, destination, date, time, size, duration or type of communication made by telephone, computer system or through any other means of communication. Similarly, video, audio or photography surveillance in private spaces means photographing people, observing or recording their conversations, movements or other activities in private spaces, and locating or tracking them via GPS or other technical means of surveillance consists in the use of devices that determine the location of the person or the object to which it is attached.

Next, paragraphs (5), (6), (7), (8), (9) and (10) define the notions of search of postal items, "monitoring of financial transactions", "detection of a corruption offence", "establishing the conclusion of an agreement", "supervised delivery" and technical supervision [18], this last notion being defined by referral rules, indicating the techniques that fall within its scope, namely:

a) interception of conversations and communications;
b) video, audio or photography surveillance in private spaces;
c) locating or tracking by GPS or by other technical means of surveillance, respectively;
d) monitoring of financial transactions and disclosure of financial data.

Taking the considerations found in the foundation of the ECHR decisions , as well as the theoretical developments of the doctrine, the editors of the Project propose that the surveillance techniques be ordered by the judge of rights and freedoms when the following conditions are met:

a) there is a reasonable suspicion regarding the preparation or commission of a crime in the category of serious crimes;
b) the measure is necessary and proportional to the restriction of fundamental rights and freedoms, given the particularities of the case, the importance of the information or evidence to be obtained or the seriousness of the crime;
c) the evidence or the location and identification of the suspect or the defendant could not be obtained in any other way or obtaining them would involve special difficulties that would prejudice the investigation or there is a danger for the safety of people or valuable goods.

Under the conditions shown, technical surveillance may be ordered regarding the suspect or defendant. As an exception, the interception of conversations and communications, as well as the location or GPS tracking, may also be ordered with respect to another person if there is a reasonable suspicion that he or she receives or transmits communications from the suspect or the defendant or intended for the suspect or the defendant, that the suspect or the

[18] Ivan Anane, *Elements of computerized records of the person*, Pro Universitaria Publishing House, Bucharest, 2015

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

defendant uses the phone or the communication system of the respective person, or their access point to a computer system, and video, audio or photography surveillance in private spaces may be ordered with respect to a person other than the suspect, if there is a reasonable suspicion that through such a measure it will be possible to discover the whereabouts of the suspect or defendant.

Regarding the monitoring of financial transactions and the disclosure of financial data, it will be possible to dispose of the person who participated or participates in the financial transactions of the suspect or the defendant, or the person who coordinates the financial activities of the suspect or the defendant.

Regarding the category of crimes for the proof of which the special techniques shown can be used, the Project uses two delimitation criteria:

1. list examples of certain criminal acts (crimes against national security provided for by the Penal Code and other special laws, drug trafficking crimes, arms trafficking, human trafficking, acts of terrorism, money laundering, counterfeiting of coins or other values, forgery of electronic payment instruments, blackmail, rape, deprivation of liberty, tax evasion, corruption crimes, crimes against the financial interests of the European Union and crimes committed through computer systems or electronic means of communication) [19];
2. the amount of the penalty, in the case of other crimes for which the law provides a penalty of 5 years in prison or more

III.2. Authorization and execution of the mandate

As an exception, the prosecutor will be able to authorize, for a maximum duration of 48 hours, technical surveillance measures when:

1. there is an emergency, and obtaining the technical supervision mandate in the usual procedure would lead to a substantial delay in investigations, to the loss, alteration or destruction of evidence, or would endanger the safety of the injured person, the witness or their family members;
2. the conditions stipulated by the normative act for issuing the mandate are met.

Similarly, the prosecutor's order authorizing the technical surveillance measure will have to include the specific terms of the mandate.

The prosecutor will have the obligation to notify, within no more than 24 hours from the expiry of the measure, the judge of rights and liberties from the court that would have the competence to judge the case at first instance or from the corresponding court at its level, in whose district is the headquarters of the prosecutor's office, of which the prosecutor who issued the ordinance is a part, in order to confirm the measure, submitting at the same time a summary report of the technical supervision activities carried out and the case file.

If the judge of rights and liberties considers that the conditions provided for in the draft normative act have been met, he will confirm the measure ordered by the prosecutor, by conclusion, pronounced in the council chamber, without summoning the parties, and in the opposite case, he will deny it, ordering, at the same time, the destruction of the evidence obtained pursuant to it, the conclusions not being subject to any appeal.

The prosecutor will personally execute the technical supervision or may order that it be carried out by the criminal investigation body or other specialized state bodies, including with the support of the competent authority.

[19] Gheorghe Buzescu, *Peculiarities of contraventional law*, Sitech Publishing House, Craiova, 2017

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

As in the current regulation, the persons who will be called to give a technical contest for the execution of the surveillance measures will have the obligation to keep the secret of the operation carried out, the violation of this obligation being punished according to the criminal law. In the same way, the data resulting from the technical surveillance measures will be able to be used in another criminal case if conclusive and useful data or information will result from their content regarding the preparation or commission of another crime from those provided for in the draft normative act.

If the grounds that justified the measure will no longer exist, the prosecutor will have the obligation to immediately stop the technical supervision before the expiration of the term of office, immediately informing the judge who issued the authorization act .

The data resulting from the surveillance measures that will not concern the fact that forms the object of the investigation or that will not contribute to the identification or location of the persons or if they will not be used in other criminal cases, will be archived at the prosecutor's office, in special places, in a sealed envelope , with the assurance of confidentiality, and may be transmitted to the judge or the panel charged with resolving the case, upon his request. At the final settlement of the case, they will be destroyed by the prosecutor, who will draw up a report to this effect.

III.3. Centralization of interceptions

Subchapter III.3 of the project, called Centralization of interceptions, [20]offers the possibility of requesting the preservation of computer data or data from telecommunications systems.

Therefore, under the conditions in which there will be reasonable suspicions regarding the preparation or commission of a crime, for the purpose of gathering evidence or identifying the suspect or the defendant, the prosecutor will be able to order the immediate preservation of computer data or data related to information traffic, or the data regarding the traffic from the telecommunications systems, being the imminent danger of their loss or modification.

The measure will be ordered by the prosecutor, ex officio or at the request of the criminal investigation body, for a maximum duration of 90 days, through an ordinance that will have to include:

- person or service provider in possession of the computer data;
- the name of the suspect or defendant, if known;
- the motivation for fulfilling the legal conditions;
- the duration for which it was issued;

The measure of preservation may be extended for "substantially justified reasons", by the prosecutor only once for a maximum duration of 90 days. The prosecutor's order will be sent, immediately, to any service provider or any person in possession of the data of interest or who has them under control, being obliged to preserve them immediately, under confidentiality conditions. If the data related to the information traffic will be in the possession of several service providers, the service provider in possession or under the control of which the computer data is will have the obligation to immediately make the information available to the criminal investigation body necessary to identify the other service providers, in order to know all the elements of the communication chain used.

[20] Gheorghe Buzescu, *The place and role of the civil servant in the state apparatus*, Sitech Publishing House, Craiova, 2017

Eximia Journal
Vol. 12, 375-388, August, 2023
ISSN: 2784-0735
www.eximiajournal.com

Within the terms indicated by the prosecutor who supervises or carries out the criminal investigation, he will order the lifting of the preserved data from the person or the service provider who owns them, or he will order the lifting of this measure.

As in the matter of technical supervision, until the end of the criminal investigation, the prosecutor will be obliged to "know" [21]in writing the persons against whom the criminal investigation is carried out and whose data have been preserved.

BIBLIOGRAPHY

Ivan Anane, *Elements of computerized records of the person*, Pro Universitaria Publishing House, Bucharest, 2015;

Ivan Anane, *The Investigation and tracking of criminals*, Pro Universitaria Publishing House, Bucharest, 2014;

Ivan Anane, *Elements of criminal procedural law,* Pro Publishing House University, Bucharest, 2015;

Ivan Anane, *Elements of Theory and Tactics of the Pursuing of Criminals*, Pro Universitaria Publishing House, 2014;

Aroveanu Adrian, Criminal Procedural Law, general part, CH. Beck Publishing House, Bucharest 2011;

Gheorghe Buzescu, *Theory Rules and practice for police usage*, Pro Universitaria Publishing House, Bucharest 2016;

Gheorghe Buzescu, *Elements of Public Order*, Pro Universitaria Publishing House, Bucharest, 2016;

Gheorghe Buzescu, *Police Law - university course*, Sitech Publishing House, Craiova, 2019;

Gheorghe Buzescu, *The place and role of the civil servant in the state apparatus*, Sitech Publishing House, Craiova, 2017;

Gheorghe Buzescu, *Peculiarities of contraventional law,* Sitech Publishing House, Craiova 2017;

Grigore Theodoru, *Treatise on Criminal Procedural Law, 2nd Edition*, Hamangiu Publishing House, Bucharest, 2008;

Grigoraş Cătălin and Adrian Petre, *Audio and audio-video recordings*, C. H. Beck Publishing House, Bucharest 2010;

Jidovu Nicu, Criminal procedural law, 2nd edition, C. H. Beck Publishing House, Bucharest, 2007;

Julean Dorel L., *Criminal procedural law – general part*, West University Publishing House, Timisoara, 2010;

Neaţă Eugen, Pruteanu Mihai, *Elements of police tactics and operational procedures regarding the intervention of public order and safety structures*, Hamangiu Publishing House, Bucharest, 2013;

Stancu E., *Treatise on Forensics revised and added*, Universul Juridic Publishing House, Bucharest, 2002.

[21] Ivan Anane, *Elements of criminal procedural law Elements of computerized records of the person*, Pro Universitaria Publishing House, Bucharest, 2015