THE 16TH EDITION OF THE INTERNATIONAL CONFERENCE
EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES

Practical Aspects Regarding the Involvement of the Romanian Intelligence Service in Criminal Investigation Files - When the Technical Support Acquires the Value of a Criminal Investigation Act

Andrei Apostol[1]

Abstract: In the light of the Decisions no. 51 of 16-th of February 2016, respectively no. 26 of 16-th of January 2019 of the Constitutional Court of Romania, the national courts were invested with researching the manner in which the technical surveillance mandates were executed. Specifically, the defenders of the persons whose conversations were recorded requested to verify whether the technical surveillance mandates were executed by a competent authority. Nationwide, there was outlined a practice of the National Anticorruption Directorate to answer the questions addressed by the courts in the sense of specifying whether the Romanian Intelligence Service provided a simple technical support in the criminal investigation activity, without carrying out criminal investigation acts. The defense of the National Anticorruption Directorate was based on the fact that the technical support does not concretely imply a criminal investigation activity, aspect that was also held by the Constitutional Court of Romania by its Decision no. 26 of 16-th of January 2019, paragraph no. 155. The notion of "technical support" is a very vague one, being necessary a distinction between the simple provision of logistic support in order to execute the technical surveillance mandate by the competent body and the support of the Romanian Intelligence Service agents in the stage of obtaining evidence through the evidentiary procedure of interception and recording of telephone calls/ conversations. This paper aims to highlight, by means of examples from the national judicial practice, the cases in which the "technical support" provided by the Romanian Intelligence Service acquires the valence of a procedural act that must be sanctioned with absolute nullity.

Keywords: Romanian Intelligence Service; technical support; technical surveillance logistics

1. The Manner of Conducting the Wiretapping Prior to the Publication of the Decision of the Constitutional Court no. 51 dated 16-th of February 2016

According to the legal literature, *"eavesdropping means intercepting, accessing, monitoring, collecting or recording communications made by telephone, computer system or any other means of communication"* (Gradinaru, 2014, p. 31).

Wiretapping has also been defined by doctrinaires as *"the intervention of authorized bodies in any kind of telephone conversations or communications or in any electronic means of communication, which involves the idea of confidentiality between those who perform it"* (Theodoru, 2007, p. 397).

The National Center for Interception of Communications (C.N.I.C.) is a military unit within the Romanian Intelligence Service with a national coverage area.

The system has national coverage and ensures the taking over of the traffic of any qualified agent in operating a network or in providing authorized telecommunications services (Gradinaru, 2016).

[1] Lawyer, Iasi Bar, Romania, Address: 2 Sf. Lazar Str., Iasi, Romania, Corresponding author: apostol.andrei93@yahoo.com.

After obtaining the authorizations, the other state institutions addressed the Romanian Intelligence Service for carrying out technical surveillance mandates (Gradinaru, 2015).

Both the founding act, the attributions, and the way of controlling the C.N.I.C. are regulated by secret decisions of the Superior Council of National Defense, so that the technical capabilities of this military unit are unknown.

According to art. 2 letter b) and art. 6 para. 2 of Protocol no. 9331 of 7-th of December 2016 regarding the cooperation between the Romanian Intelligence Service and the Public Ministry for establishing the concrete conditions for access to technical systems of the National Center for Communications Interception:

The Romanian Intelligence Service ensures to the Public Ministry, its central or territorial structures, as well as to the criminal investigation bodies delegated by the prosecutor, direct and independent access to technical systems owned and managed by it, through the National Center for Interception of Communications, for enforcing the authorization documents issued pursuant to the provisions of the Criminal Procedure Code or of a special law, purpose for which:

b) it makes available to the Public Ministry the computer applications held by the National Center for Interception of Communications in order to request from the electronic communications operators directly and independently the traffic data, under the conditions provided by the special law;

"Art. 6 para. 2: Upon request, the National Communications Interception Center provides the necessary support for the identification of the technical interception solution, in the case of communications operators that do not have an active interception function.''

Reading these provisions, we can observe that the C.N.I.C. allows the interception of communications within a centralized system.

According to art. 5 of Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector, traffic data relating to subscribers and users, processed and stored by the provider of a public electronic communications network or by the provider of a electronic communications service intended for the public, must be deleted or transformed into anonymous data, when they are no longer necessary for the transmission of a communication.

This Law allows the mobile telephony operators to store traffic data from their users in order to establish the contractual obligations of their subscribers

The processing of traffic data can be carried out for a maximum of 3 years from the due date of the corresponding payment obligation.

Thus, the mobile telephony operators store the traffic data in encrypted form, containing the subscriber calls for a period of up to 3 years.

The processing of traffic data may be performed only by persons acting under the authority of providers of public electronic communications networks or electronic communications services intended for the public, having as attributions invoicing or traffic management, customer relations, fraud detection, marketing electronic communications services or the provision of value-added services, and is allowed only to the extent necessary for the performance of these duties.

By communication we understand *any information exchanged or transmitted between a certain number of participants through an electronic communications service intended for the public*[1]*;*

Traffic data is defined as*"any data processed for the purpose of transmitting a communication through an electronic communications network or for the purpose of invoicing the counter value of such operation"*[2].

Thus, the mobile telephony operators store the traffic data of its subscribers on their own equipment.

According to sheet 8 of the report dated 5-th of February 2021 regarding the verification performed by the President of the High Court of Cassation and Justice pursuant to art. 301 of Law no. 304/2004 on judicial organization, republished, with subsequent amendments and completions:*The technical processes of eavesdropping are performed by means of equipment from the centers of telecommunications operators, and the content of intercepted communications is transferred fully automated to the storage system managed by the National Center for Interception of Communications, without any human intervention from the staff within the Romanian Intelligence Service.*

Of course, the report takes into account the context following the publication of the decision no. 51/2016of the Constitutional Court, but there is no reason to believe that the principle of achieving the wiretaps through the National Center for Communications Interception has been changed.

Hence, staff within the National Interception Center had access to the equipment of the mobile telephony operators in which the traffic data of the subscribers were stored (Gradinaru, 2017, p. 88).

Following the issuance of the technical surveillance mandate, the prosecutor ordered the delegation of its enforcement to the workers within the Romanian Intelligence Service. The technical surveillance mandate contained relevant data for the identification of the target terminal: telephone number, the network operator providing the mobile telephony services, the IMEI[3] (identification number of the terminal), etc.

According to art. 34 para. from Protocol no. 00750 of 4-th of February 2009 concluded between the Romanian Intelligence Service and the Public Ministry, the Romanian Intelligence Service shall ensure the recording of communications or conversations resulting from interception on serial data media, provided by the prosecutor, as well as their sending to the Prosecutor's Office or to the Territorial Prosecutor's Office concerned.

The Service could also ensure the transcription of the communications or conversations considered relevant in the case.

Also, at the written request of the prosecutor, the Service may ensure the rendering of other conversations, selected from the recorded traffic. The request must contain the number of the authorization act, the interception criterion (telephone number, IMEI series of the mobile terminal, IP address, radio frequency), the date and time of the call or communication. In order to carry out these activities, the Prosecutor's Office or the territorial prosecutor's offices will send to the Service data supports containing the records previously obtained.

Based on the data mentioned in the technical surveillance mandate and through the National Interception Center, the target terminal was established.

[1] Article 2 para. 1 letter d) of Law no. 506/2004.
[2] Article 2 para. 1 letter b) of Law no. 506/2004.
[3] International Mobile Equipment Identity.

Pursuant the above identification data, *"the raw content of the communication is recorded, extracted and transferred automatically from the communications operator to the storage system managed by C.N.I.C., without any human intervention being possible on the communication flow"* (Suian, 2021, p. 224).

Drafting of conversation rendering notes, decryption of obtained data, selection of calls, storage of data on optical media were activities performed by workers within the Romanian Intelligence Service (S. Gradinaru, Some remarks on the expertise of media containing the results of the technical surveillance activity, Journal of Criminology, Criminalistics and Penology No. 1-2 / 2012, p. 119).

However, the conversation rendering notes were not attached to the case file, the criminal investigation body making its own transcripts (Gradinaru, 2020).

We consider that this practice was meant to hide the involvement of the secret services in the criminal investigation activity.

Together with the publication of the Constitutional Court's Decision no. 51/2016 in the Official Journal, the involvement of the employees within the Romanian Intelligence Service in the technical surveillance mandates enforcement, represents an activity carried out outside the legal framework.

We appreciate that any direct activity of the Romanian Intelligence Service workers, even based on a delegation ordinance from the prosecutor, regardless of whether it concerns decryption, storage of data on optical media, selection of conversations, drafting of operative notes, represents a criminal investigation act drawn up by a body that lacks jurisdiction (Gradinaru, 2013, p. 78).

Even prior to the Constitutional Court's Decision no. 51/2016, it was pointed out that it is forbidden for the prosecutor to delegate to the employees of the Romanian Intelligence Service the activities of rendering the recordings of telephone conversations (Gradinaru, 2014, p. 119).

Likewise, we agree with the opinion according to which the results of the technical surveillance carried out under the conditions shown above would represent an *extrajudicial* evidence, being administered in the absence of the case prosecutor, thus, art. 102 para. 2 of The Criminal Procedure Code shall be applicable (Gradinaru, 2014, p. 69).

2. The Manner of Conducting the Interceptions of Telephone Conversations Following the Publication of the the Constitutional Court's Decision no. 51 dated 16-th February 2016.

According tothe explanatory memorandum of the Emergency Ordinance no. 6 of 14th March 2016:

taking into account the fact that the activity of the prosecutor's offices would be seriously affected in the absence of technical support and specialized human resources for the management of a communications infrastructure, both from the point of view of the efficiency of criminal prosecution and in terms of taking of complete evidence based on all methods of investigation provided by Law no. 135/2010 on the Criminal Procedure Code, as subsequently amended and supplemented,

Subsequent to the publication of the Constitutional Court`s Decision no. 51 of 16-th of February 2016 in the Official Journal, the National Prosecutor's Offices faced real difficulties in the enforcement of thetechnical surveillance mandates both for logistical and personnel reasons.

We will reference again to Protocol no. 00750 of 4-th of February2009 concludedbetweenthe Romanian Intelligence Service andthe Public Ministry (in force prior to the judgement no. 51 of 2016) whose

provisions were analyzed throughout the Constitutional Court's Decision no. 26 of 2019 published in theOfficial Journal no.193 dated 12-th of March 2019.

According to art. 60 of the above Protocol: *The parties will ensure the acquisition, thorough knowledge and the effective enforcement of the provisions of the protocol by their own staff, including by the territorial prosecutor's offices and the county intelligence directorates, in relation to the tasks devolved to them in their application.*

Related to these provisions and from the corroboration of all the provisions of the protocol, we consider that its application did not belong to the Prosecutor's Offices, but subsequently to obtaining a technical surveillance mandate, based on the protocol, the prosecutor had the obligation to notifyt he Romanian Intelligence Service, in order to enforce the technical surveillance measure consisting in intercepting telephone conversations.

The above finding is also reinforced by the Report on the conclusions and proposals of the Permanent Joint Commission of the Chamber of Deputies and the Senate for exercising parliamentary control over the activity of the Romanian Intelligence Service in connection with the "Report on theactivity of the Romanian Intelligence Service during 2016": *Until 2016, the Romanian Intelligence Service was the only institution that, due to the advanced technical infrastructure and specialized human resources, ensured the enforcement of all measures authorized by law to restrict certain civil rights and freedoms.*

The competence was granted to the Service by acts having the legal force of an administrative act, but which are mandatory for the authorities refered to, respectively HCSAT no. 0068/2002 on the development of the National Communications Interception System, intended for the enforcement of authorization documents, as well as HCSAT no. 0029/2008 regarding some measures required for the operationalization and development of the National Communications Interception System. This state of affairs ceased in 2016, as a consequence of the adoption of Decision no. 51/2016 of the Constitutional Court of Romania.

For the above-mentioned reasons, the situations in which the Technical Service within the National Anticorruption Directorate, the General Anticorruption Directorate or the Special Operations Directorate or the Information and Internal Protection Directorate implemented the technical surveillance mandates consisting in intercepting calls were not to be found in judicial practice.

Another obstacle faced by the Prosecutor's Offices in the enforcement of technical surveillance measures consisting in intercepting calls is the fact that they could not access the National Communications Interception Center without the assistance of Romanian Intelligence Service workers.

Under such circumstances, the activity of implementing the technical surveillance mandates could not be put in agreement with the Constitutional Court's Decision no. 51/2016 provisions.

On these grounds, the Emergency Ordinance no. 6 of 14-th of March 2016 regarding some measures for the enforcementof technical surveillance mandates ordered incriminal trials, where art. IV provides the following: *The concrete acces conditions to the technical systems of the judicial bodies are established by cooperation protocols concluded by the Romanian Intelligence Service with the Public Ministry, the Ministry of Internal Affairs, as well as with other institutions within which special criminal investigation bodies operate under art. 57 para. (2) of the Criminal Procedure Code.*

Such a protocol was concluded on 7-th of December 2016 (Protocol no. 9331 on cooperation between the Romanian Intelligence Service and the Public Ministry for establishing the concrete access conditions to technical systems of the National Center for Communications Interception).

According to art. 2 of the previously mentioned protocol: The Romanian Intelligence Service ensures to the Public Ministry or to the criminal investigation bodies delegated by it, the direct and independent access to the technical system of interception, in order to implement, in a centralized system, the technical surveillance mandates.

Art. 3 of the Protocol provides: *The access of the Public Ministry to the technical systems provided in art. 1, letter a) is done directly and independently by:*

a) the use of specific interception computer applications;

b) the management of targets and technical surveillance mandates;

c) the management of the users within the structure connected to the system;

d) directing the intercepted signal and / or receiving it to / fromstructures established by the Public Ministry;

e) the export of intercepted products through specific computer applications.

With the signing of protocol no. 9331 concluded between the Public Ministry and the Romanian Intelligence Service, in order to access C.N.I.C, equipment belonging to the National Anticorruption Directorate, the Directorate for the Investigation of Organized Crime and Terrorism, the General Anticorruption Directorate and the Special Operations Directorate was ensured.

Thus, the prosecutor or the judicial police officers delegated with the enforcement of the technical surveillance mandate will be able to access the National Interception Centerthrough a computer system, and the latter will collect and store the intercepted communications on their own servers (M. Suian, Special methods of surveillance or research, Solomon Publishing House, 2021, p. 202).

Data stored on C.N.I.C. will only be accessible to the person enforcing the technical surveillance mandate, hence excluding the intervention of Romanian Intelligence Service workers (according to file 8, para. 5 of the report on the verification performed by the President of the High Court of Cassation and Justice under art. 301 of the Law No. 304/2004 on judicial organization, republished, with subsequent amendments and completions no. 1314 of 14-th of May 2020).

We can note that between the date of publication of the Constitutional Court's Decision no. 51/2016 in the Official Journal and the date on which Protocol no. 9331 (7-th of December 2016) was signed, it passed an important period of time in which technical surveillance mandates consisting in wiretapping were enforced.

Hereinafter, we will submit for discussion the legality of the evidence obtained through the technical surveillance methods implemented between 14-th of March 2016 and7-th of December 2016.

3. Invoking the Unlawfulness of the Technical Supervision Mandates Acts of Implementation by Bodies that Lack Jurisdiction

In a case pending before the Iasi Court of Appeal, it was found that in the criminal investigation phase, evidence obtained by the approval of technical supervision measuresbased on the warrants issued by the judge of rights and freedoms within the Iasi Housecourt was administered, namely:

Throughout the prosecution volume, minutes drawn up by workers within The General Anticorruption Directorate who transcribed the intercepted telephone conversations can be identified.

The sole order of delegation to the officers of the General Anticorruption Directorate by the case prosecutor, found in the case file is dated 22-nd of April 2016, and the GAD officers are requested to transcribe the recordings made based on the technical surveillance mandates.

This situation attracted the attention of the defense, which requested additional information from the prosecution regarding the body that enforced the technical surveillance mandates.

In the response of the Prosecutor's Office attached to the Iasi Courthouse, the latter mentioned the fact that the technical surveillance mandates were implemented by the staff within The Special Operations Directorate.

Considering that the case file lacked information on the body that enforced the technical surveillance mandates, the defense requested the issuance of addresses to the Special Operations Directorate, respectively to the Romanian Intelligence Service for these institutions to specify whether they were involved or not in the activity of implementing the technical surveillance mandates.

Equally, the Special Operations Directorate was requested to clarify whether between the 14-th of March 2016 and the 7-th of December 2016, it wielded the necessary technical equipment to intercept telephone calls.

The request for evidence was based on the fact that the National Communications Interception Center within SRI is the only entity that owns and manages the nationwide unique technical infrastructure for the interception and recording of electronic communications.

According to Decision no. 51/2016 (paragraph 34) by which the court of constitutional contentious qualified the activities provided in the second thesis of para. 1of art. 142 of the Criminal Procedure Code as evidentiary proceedings in criminal trials: *The Court concludes that the acts performed by the bodies provided in the second thesis of para. 1 of art. 142 of the Code of Criminal Procedure, represent the evidentiary proceedings that are the basis of the report of the technical surveillance activity, which constitutes a means of proof.For these reasons, the authorities that can participate in their implementation are only the criminal investigation bodies).*

It was ruled by the Romanian Constitutional Court that the implementation of technical surveillance should be carried out only by the judicial bodies, thus motivating (in paragraph no. 49) that this activity can be performed by "specialized workers within the police, in the conditions in which they can hold the approval attesting their quality of judicial police officers, under art. 55 para. 5 of the Criminal Procedure Code."

Regarding the phrase *"persons who are called to give technical assistance in the enforcing of surveilance measures"*within art. 142 para. 3 of the Criminal Procedure Code, it refers to the entry of the data provided in the warrants issued by the judge of rights and freedoms into the fixed / mobile telephony operators' control panels, followed by the extraction, selection, recording and storage of the results obtained (activity performed exclusively by specialists within the National Center for Interception of Communications belonging to SRI as owner / administrator of the National Interception System).

Therefore, the interception of communications (as a special method of surveillance or research) was performed exclusively through the system managed by SRI, given that the General Anticorruption Directorate (GAD) does not have the necessary technical infrastructure to connect directly to telecommunications service operators, so that it can perform independently intercepts/ records of telephone conversations.

The lack of jurisdiction, whether it is considered from a material or functional point of view, concerns both the procedural acts of criminal investigation, and those to be performed as a preliminary (Gradinaru, 2014, p. 65).

Under these conditions, the effective enforcement of the technical surveillance mandates provided by art. 142 para. 1 of the Criminal Procedure Code, as a probative procedure, was carried out with the involvement of officers within SRI, who proceeded to intercept communications (for the purposes of art. 138 para. 1 letter a) and para. 2 of the Criminal Procedure Code) and not with specialized workers within the Special Operations Department, to whom the acoustic signal stored on the optical media was subsequently transmitted in order to proceed to its rendering.

Given that the system of interception / recording of conversations / communications used in gathering evidence belongs to SRI, the legal provisions on the implementation of technical surveillance measures consisting in intercepting communications, respectively video, audio or photography surveillance were violated, all the activities being carried out by bodies without criminal investigation attributions.

Through the address dated 17-th of May 2021, the Special Operations Department claimed that the Romanian Intelligence Service did not provide technical support in the execution of the technical surveillance mandates, and this unit has the necessary equipment for enforcing the technical surveillance mandates.

On the other hand, the Romanian Intelligence Service stated the opposite, respectively that it partially provided technical support in intercepting telephone conversations.

The answers given to these addresses were evasive and contradictory. The Special Operations Department stated that it currently has the necessary equipment for intercepting telephone calls, although it was asked strictly about the period between the 14-th of March 2016 and the 7-th of December 2016.

At the same time, the Romanian Intelligence Service did not answer whether or not the technical support provided involved human intervention on the part of a worker within it.

We appreciate that additional clarifications are needed from government institutions, in order to guarantee the right to defense and a fair trial.

National courts have the obligation to conduct an effective and efficient judicial investigation, in particular as regards the verification of the manner in which the technical surveillance mandates have been enforced.

The interception of communications (as a special method of surveillance or investigation) was carried out exclusively through the system managed by SRI, given that the Special Operations Directorate did not have the necessary technical infrastructure to connect directly to telecommunications service operators, so that they can perform independently.

According to art. 8 of Law no. 14/1992 on the organization and functioning of the Romanian Intelligence Service, *"The concrete conditions for access to the technical systems of the judicial bodies are established by cooperation protocols concluded between the Romanian Intelligence Service and the Public Ministry, the Ministry of Internal Affairs, as well as other institutions within which special criminal investigation bodies operate, under art. 57 para. (2) of the Criminal Procedure Code".*

The above paragraph was introduced by point 1 of the Emergency Ordinance no. 6/2016 starting with the 14-th of March 2016.

In the present case, the technical surveillance mandates were issued on 1-st of April 2016.

Protocol no. 9331 regarding the cooperation between the Romanian Intelligence Service and the Public Ministry for establishing the concrete conditions for access to technical systems of the National Center for Communications Interception was concluded on the 7-th of December 2016.

Therefore, in the period between March and May 2016 there were no conditions for access to the technical systems of the National Center for Interception of Communications by the Iasi Special Operations Service.

The access to the National Center for Interception of Communications could be made only through the Romanian Intelligence Service, as recognized by this institution through the address submitted to the case file, in which it states that it provided technical support to the criminal investigation bodies.

Transmission of the signal from the C.N.I.C. it could be achieved only by the intervention of an employee within the Romanian Intelligence Service.

The National Center for Interception of Communications is a military unit within the Romanian Intelligence Service.

Any operation performed at the headquarters of the C.N.I.C. requires an authorization from the S.R.I., as well as the presence of an employee of the Service for accessing the computer system.

The technical support consists in the "transmission of the signal" from the C.N.I.C., thus implying the support of a SRI worker who will access the computer system and will direct the mobile traffic data to the Special Operations Directorate.

The National Center for Interception of Communications is a military unit within the Romanian Intelligence Service.

The direct involvement of a SRI worker (who is not a criminal investigation body) in the activity of enforcing the technical surveillance measure determines the annulment of all the results of the technical surveillance activity (Gradinaru, 2018, pp. 5-22).

The fundamentally different nature of the criminal investigation bodies from that of the Romanian Intelligence Service, in terms of compliance with individual guarantees in a democratic society requires the non-involvement of the latter (Gradinaru, 2017, p. 96).

4. Judicial Practice that Supports the Idea that the Technical Support Provided by SRI Workers Regarding the Acts of Implementation of Technical Surveillance Measures Determines the Absolute Nullity of the Results of Technical Surveillance

The national courts appreciated the fact that the technical support provided by SRI was in fact a real criminal investigation. In this sense, we reproduce the considerations of the conclusion of the judge of the preliminary chamber from 18.12.2020 from the file no. 3813/99/2018/a1: *Even if the claims of the criminal investigation body, as well as those of SRI take into account and emphasize the involvement of the intelligence service exclusively at the level of "technical support", this activity has the legal nature of a procedural act by which the processual act legally issued by the competent court was executedand it results in a presumed harmrelative to the exercise of the fundamental rights of the persons concerned, so that the sanction of absolute nullity becomes incident.*

The Iasi Court of Appeal also had a similar argument in judgement of 19-th of February 2021 in file no. 2192/89/2015 *Even if the involvement of S.R.I. is confined to the level of technical support, this activity has the nature of a procedural act by which the processual act by which the interference in private life*

was approved is enforced and is directly related to obtaining evidence through the probative procedure of technical surveillance. As the execution of the technical supervision measures was to be carried out only by the prosecutor or by the criminal investigation bodies of the judicial police, the sanction of absolute nullity will be incidental even if the criminal investigation bodies subsequently legally performed some processual activities by who they "validated" the results of the illegally enforced technical surveillance (Iasi Court of Appeal, judgement of 19-th of February 2021 in file no. 2192/89/2015).

We also note the case law of the High Court of Cassation and Justice: *All surveillance measures were implemented with the technical support of the Romanian Intelligence Service, meaning that the Romanian Intelligence Service provided the necessary infrastructure to implement the respective technical surveillance measures, which is equivalent to the involvement of the Romanian intelligence service in the activity of criminal investigating, more precisely, in the stage of obtaining evidence through the probative procedure of interception and recording of telephone and environmental conversations / communications.*

Violation of the provisions of art. 142 para. (1) 2-nd thesis of the Criminal Procedure Code consisting in the enforcement of surveillance measures by bodies other than the prosecutor or criminal investigation bodies of the judicial police, attracts the absolute nullity of the acts thus performed, by applying art. 281 para. (1) lit. b) of the Criminal Procedure Code - in the form established as constitutional by Constitutional Court's Decision no. 302/2017. This conclusion is also found in the recent jurisprudence of the High Court of Cassation and Justice (criminal decision no. 92 of 30-th of May 2018 of the High Court of Cassation and Justice, Panel of 5 judges). (...)

Following the finding of the nullity of the probative procedure, the nullity of the evidence thus obtained will be ascertained, so that, pursuant to art. 102 para. (2) - (4) of the Criminal Procedure Code, it is necessary to exclude from the evidentiary material all the minutesrecording the results of the technical surveillance activities. (High Court of Cassation and Justice, Criminal Section, panel of 2 preliminary chamber judges, conclusion no. 31 / C of 27-th of September 2018).

5. Conclusions

The issue of the jurisdiction to carry out the acts of enforcing the technical surveillance mandates continues to represent a problem of interest for the national courts.

The technical specificity of the criminal investigation acts to which the SRI workers provided logistical support to the criminal investigation bodies may determine erroneous solutions in the judicial practice.

For these reasons, it is necessary that the national courts pay more attention in conducting the judicial investigation in the criminal cases in which telephone interceptions were carried out in the period prior to the signing of Protocol no. 9331 dated 7-th of December 2016.

At the same time, the practice of the Prosecutor's Offices to try to diminish the role of SRI's involvement in criminal prosecution cases under the pretext that the support provided in conducting telephone interceptions is exclusively technical must be viewed by national courts from a technical perspective.

If the technical support consists in transmitting the signal from the C.N.I.C. to the technical service of the criminal investigation bodies, then the national courts will find the direct involvement of a worker within the S.R.I. (who does not have the quality of a criminal investigation body) in the activity of criminal investigation and will sanction with absolute nullity the results of the technical surveillance.

If the technical support consists in making available to the Prosecutor's Offices the logistics necessary to carry out the telephone interceptions that would allow direct and without human intervention access to the C.N.I.C. (situation not encountered in practice prior to the Constitutional Court's Decision no. 51/2016 and respectively prior to the signing of Protocol no. 9331 of 7-th of December 2016), the courts will ascertain the legality of the results of technical surveillance from the perspective of the jurisdiction of the criminal investigation body involved.

6. References

Theodoru, G. (2007). *Treaty of criminal procedural law*. Bucharest: Hamangiu, p. 397.

*** (2018). *The High Court of Cassation and Justice, Criminal Section, panel of 2 preliminary chamber judges*, judgement no. 31 / C of 27-th of September 2018.

*** (2004). Law no. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector.

Suian, M. (2021). *Special methods of surveillance or research*. Bucharest: Solomon.

Gradinaru, S. (2013). Aspects in connection to the interception and the recording of talks or conversations performed under the provisions of the Law 51/1991 regarding the national security of Romania. *EIRP Proceedings,* Galati: Editura Universitara Danubius.

Gradinaru, S. (2017). *Usage of interceptions and audio or video recordings as evidence in criminal proceedings and compatibility of regulation with European and international requirements.* Presa Universitara Clujeana Publishing House.

Gradinaru, S. (2014). *Technical Surveillance in the New Criminal Procedure Code*. C. H. Beck Publishing House.

*** (2020). *Iasi Courthouse, judgement of the judge of the preliminary chamber* from 18-th of December 2020 in the file no. 3813/99/2018/a1.

*** (2009). *Protocol no. 00750* of 4-th of February 2009 concluded between the Romanian Intelligence Service and the Public Ministry.

Romanian Constitutional Court (16 February 2016). Decision no. 51/2016 published in the *Official Journal no. 190*.

*** (2016). *Protocol no. 9331* of the 7-th of December 2016 on the cooperation between the Romanian Intelligence Service and the Public Ministry for establishing the concrete conditions for access to technical systems of the National Center for Communications Interception

Romanian Constitutional Court (12 March, 2019). Decision no. 26/2019 published in the *Official Journal no. 193*.

Iasi Court of Appeal (2021). *Judegement of 19-th of February 2021 in file no. 2192/89/2015.*

*** (2021). The report dated 5-th of February 2021 regarding the verification performed by the President of the High Court of Cassation and Justice pursuant to *art. 301 of Law no. 304/2004* regarding the judicial organization, republished, with the subsequent modifications and completions