WIRE TAPPING IN CRIMINAL TRIAL. GUARANTEES FOR A FAIR TRIAL

Radu Bogdan CĂLIN[*]

Abstract

The purpose of this paper is to carry out an examination of the national legislation and jurisprudence in order to establish whether sufficient guarantees are regulated by law against arbitrariness, for the persons who have been supervised by the state bodies. The study aims to identify possibilities of updating the legislation for its compliance with the CCR decisions and with the ECtHR jurisprudence. The evidentiary process of interception of communications is an important means by which state bodies investigate complex criminal activities, but it involves an interference with the right to privacy, so it is necessary to have substantive and procedural safeguards to prevent arbitrariness from state bodies and to ensure adequate protection of the right to privacy.

In the first part of the study, a presentation is carried out of the evolution of the Romanian legislation and an analysis of the guarantees regulated by it. In the second part, the ECtHR jurisprudence is presented regarding the guarantees that must be regulated by national legislation to respect the right to privacy and to avoid unjustified interference. In the last part of the paper, the substantive and procedural guarantees offered by national legislation and jurisprudence are presented and an analysis of their compliance with the jurisprudence of the ECtHR is carried out. In the conclusions of the paper, two proposals for updating the Romanian Criminal Procedure Code and Law no. 51/1991 on Romania's national security are introduced.

Keywords: *wire tapping, limitation of the right to privacy, history of legislation in the field of wire tapping /telephone tapping, technical surveillance, national security warrant.*

1. Introduction. Interception of conversations and communications – the genesis

The surveillance of people in order to discover and prove criminal activities was initially the prerogative of the secret services. In order to become an evidentiary procedure in a criminal trial, the surveillance methods had a winding evolution.

In the history books[1], among the first mentions of surveillance by spy agencies were the interception of Hitler's communications with his generals during the Second World War and the English decoding team at Bletcheley Park breaking the Enigma code.

In Romania, the surveillance of persons was regulated by law for the first time in 1978 as a tool of the secret services for discovering and proving criminal activities. Despite the fact that the surveillance methods were extrajudicial in nature, the materials obtained as a result of surveillance activity were used to prove criminal activities. Contentwise, the special surveillance measures as an evidentiary procedure ordered in the criminal proceedings/trial, have their source in the surveillance techniques used in espionage. The surveillance of people was initially regulated as an espionage technique that was implemented by the security bodies, and the materials thus obtained could be used in the criminal proceedings.

During the communist regime, the special methods of surveillance in the sense given today to the evidentiary procedure used in the criminal proceedings were not regulated by primary legal provisions. In the Criminal Procedure Code of 1968, adopted by the Great National Assembly on November 12, 1968, the special surveillance methods were not provided for as evidentiary procedures that could be used in criminal proceedings.

The fact that the special methods of surveillance were not regulated by the Criminal Procedure Code did not prevent the bodies of the Department of State Security from conducting mass surveillance of the population.[2]

In that period, multiple investigative methods were used for population surveillance, which in terms of content were similar to the point of overlap with special surveillance methods, but the authorisation procedure

[*] PhD Candidate, Faculty of Law, „Nicolae Titulescu" University of Bucharest (e-mail: calinradu03@gmail.com).

[1] M. Smith, *Spargerea codului nazist, Enigma*, Orizonturi Publishing House, Colecţia Secretele istoriei, 2011.

[2] The truth about the past: The invisible witness – Security and surveillance, an episode broadcast by TVR on May 9, 2021, available online *https://www.youtube.com/watch?v=m6uuCOqEc6k&ab_channel=TVR*.

was totally different and there was no guarantee against arbitrariness. The persons under surveillance of the security bodies, the only ones capable of authorising and implementing the means of surveillance, could become criminal law subjects as a result of surveillance, and the materials obtained as a result of surveillance were vital evidence on which their conviction was based.

Surveillance was carried out during the communist period by specific means, namely wiretapping, infiltration of an informer (or an officer), secret entering, secret search and informative research, means which were classified as informative-operative activities.[3]

2. Shadowing / Tailing / Stakeout - surveillance measure during the communist period

Shadowing, as a special method of investigation, was regulated by the Order of the Minister of the Interior no. 001401 of 01.07.1978[4] *„Instructions on shadowing/tailing and investigative work".* According to the order, tailing was a special means of security work, through which data, information and evidence were obtained for the purpose of preventing, discovering and neutralizing criminal activities under state security. Competence. The tailing was not an evidentiary process used in the criminal proceedings, but especially outside it, but which led to obtaining of evidence that could have been the basis of a criminal investigation and subsequently the basis of the application of a criminal sanction.

Tailing was an activity closely related to the criminal proceedings, as the main purpose of this measure was to discover and neutralize criminal activities. Tailing authorisation was very different from the procedure regulated by the Criminal Procedure Code for the evidentiary procedure of special surveillance methods, which involves a high interference in the rights of the persons subject to surveillance.

Tailing authorisation, according to art. 5 and 6 of the Order of the Minister of the Interior no. 001401 of 01.07.1978, was carried out at the request of an information subunit and was approved by the commanders of the central information units. This procedure entailed the request, authorisation and enforcement of surveillance by security bodies and offered no guarantee against arbitrariness. In order for the surveillance measure not to produce too much interference with the right to privacy and for there to be a fair balance between the general interest of the state to prove criminal activities and the right to privacy, it is necessary to have several guarantees. A first guarantee is represented by the existence of a clear and predictable legislation framework, which regulates in detail the conditions for the authorisation of the measure, the procedure which must be followed for the authorisation of the measures and the way of execution.

Tailing authorisation did not offer this guarantee. First of all, the regulatory act which regulated the measure was strictly secret, it was not brought to the public's attention through publication in the Official Gazette, it was secondary legislation - subordinate to the primary legislation and did not represent a clear and predictable law. The law did not meet the conditions of clarity and predictability, as the conditions that must be met for the authorisation of the measure were not detailed, so that a person had the possibility to foresee under which conditions they could be supervised by the state bodies.

A second guarantee consists in the existence of a real filter on the part of the state bodies, which should assess concretely, by reference to each individual case, if the conditions stated by the legislator for the authorisation of the measure are met. Tailing did not meet this condition either, and it was entirely the prerogative of the security bodies, which proposed, ordered and implemented the wiretapping measure. Tailing was ordered at the request of an informational subunit and was approved by the commander or deputy of the central informational unit. In the case of complex security actions, the execution of which required the participation of a large number of forces on a specialised line of work, the request proposing the tailing was made by the Special Tailing and Investigations Unit and was approved by the Deputy Minister, chief of the Department of State Security or his substitute on command. It is noted that the person who made the request and the person who approved it were part of the same structure, respectively they were security bodies, and between them there was a relationship of subordination. Consequently, the procedure for authorising the tailing did not comply with a minimum standard of objectivity and did not offer a guarantee against the arbitrariness of state bodies.

[3] Instructions no. D – 00190/1987 regarding the organisation and performance of the information-operative activity of the security bodies.

[4] Order of the Minister of the Interior no. 001401 of 01.07.1978 was classified as strictly secret and can be consulted at the National Council for the Study of the Securitate Archives (CNSAS) archive or online *http://www.cnsas.ro/documente/materiale_didactice/D%200087 12_001_p34.pdf*.

The third guarantee refers to the existence of a maximum period during which the state bodies can monitor/watch a person, the existence of a clear procedure for the implementation of the measure and some levers for contesting the measure. Regarding the duration of the tailing measure[5], it is mentioned that continuous tailing is carried out for a maximum duration of 5 days, intermittent tailing for a duration of up to 7 days with interruptions, tailing at operative moments for a short period of time, and study tailing over a longer period. It should be noted that the regulatory act does not regulate the possibility of extending the tailing measure. With regard to the continuous and intermittent tailing, an enforcement period of 5 days and 7 days is regulated, but for the tailing at operative moments and for the study, there is no time limitation of the measure, the issuer of the act using vague terms such as „short time" or „longer period", which can be interpreted subjectively.

Although a duration for the tailing measure execution is provided for, art. 20 para. (2) of the Order of the Minister of the Interior 001401 of 01.07.1978 provides that in cases of particular importance, the maximum duration of tailing can be extended only with the approval of the commander of the Special Detention Unit and Investigations. The previously mentioned regulatory act does not meet the requirement of clarity, as it does not regulate objective criteria by which the special importance can be assessed, nor does it limit the extent of the tailing in time, as there is no regulation of a maximum duration that cannot be exceeded in case of successive extensions. As for the duration of tailing, there was no maximum period regulated by the regulatory act during which a person could be subject to surveillance and there was no procedure for informing the person under surveillance and no way to challenge such measure.

Consequently, the fact that there was no legal procedure for ordering the tailing measure, for which there were guarantees against arbitrary interference by state bodies, led to a mass surveillance of the population during the communist regime.

Regarding the content, tailing consists in following people or surveilling buildings and places object of security work, secretly, by using specific methods, procedures and means. The information, the data obtained and the findings of the tailing agents during the pursuit or surveillance of the objectives, the result of the identifications and the documentation made materialised in tailing notes or briefings, photographs or films, reports on the performance of some preliminary acts or other means of evidence.

Analyzing the content of video and audio or photography surveillance involving photographing people, observing or recording their conversations, movements or other activities, it can be seen that in terms of content, the measure is identical to tailing. The secret photography and filming are carried out during tailing implementation in order to document the facts and activities of a criminal nature or with operational significance of the objectives, discovered by the surveillance officers or indicated by the interested security information units, to study the environments frequented by some of them or to identify some people who appear in their entourage.

A difference regarding the content of the two measures consists in the fact that video, audio or photographic surveillance as an evidentiary procedure has a person as its object of surveillance, unlike the tailing measure which could have either a person or an objective as its object of surveillance.

In the contents of the Order of the Minister of the Interior 001401 of 01.07.1978 it is stipulated that certain addresses can be monitored, and the establishment of visitors and persons domiciled at the visited addresses would necessarily be preceded by the consultation of the security information unit requesting the surveillance and their verification in tailing and investigation records. Both measures are carried out under conditions of confidentiality. Even if the legislator of the Criminal Procedure Code of 2010 does not expressly regulate that the measure of video, audio or photography surveillance is secret, in order to capture the criminal activity and the natural behaviour of the persons under surveillance, it is necessary that the measure be confidential.

The tailing measure is approved by the security bodies and is also implemented by the security bodies. Following the implementation of the tailing measure, tailing notes or briefings, tailing-identification notes, notes-reports, photographs or films, reports on the execution of some preliminary acts or material means of evidence were drawn up. It is noted that, despite the fact that tailing was not a procedural measure, based on it, evidence was obtained which was later used in the criminal trial, both the reports on the execution of some preliminary acts, as well as the material means of evidence had probative value.

[5] Art. 20 para. (1) of the Order of the Minister of the Interior no. 001401 of 01.07.1978.

Video, audio or photographic surveillance is especially useful when a proactive investigation is being carried out and criminal activity is ongoing. In these situations, the materials resulting from surveillance have a high probative value, capturing even the criminal activity. The evidentiary procedure is also useful when a reactive investigation is carried out, after the crime has been consumed and exhausted, but as a rule the materials obtained have a lower evidentiary value. With regard to the materials resulting from tailing, there was no possibility of invoking their nullity, since only the violation of the legal provisions regulating the conduct of the criminal proceedings attracted the nullity of the act, according to the Criminal Procedure Code of 1968. Given that tailing was not a measure to be ordered in a procedural framework, but a measure of extrajudicial surveillance, the nullity of the materials resulting from tailing could not be invoked.

With regard to the accessibility of the Order of the Minister of the Interior 001401 of 01.07.1978, considering its classification as a state secret - strictly secret and the consequences deriving from this classification, namely the incurring of criminal liability for disclosing the information contained in the act, the regulatory act was not made public. Not only that the Order of the Ministry of the Interior 001401 of 01.07.1978 was not published in any regulatory act, and its content was not brought to public knowledge, but it was classified as strictly secret, and its content could only be known by the state bodies who had authorisation to access classified information. In the case of disclosure of its content, criminal liability could be incurred for committing the crime of disclosure of a secret which endangered the security of the state.[6]

According to the rich ECtHR jurisprudence, the accessibility and predictability of the law are two particularly important qualities that a law must fulfil, and it established a series of criteria by reference to which it is analyzed whether a law is accessible and predictable. In cases such as *Sunday Times v. United Kingdom of Great Britain and Northern Ireland*, 1979, *Rekvényi v. Hungary*, 1999, *Rotaru v. Romania*, 2000, *Damman v. Switzerland*, 2005, ECtHR emphasised that „it cannot be considered - law- other than a norm stated with sufficient precision, to allow the individual to regulate his/her conduct. The individual must be able to foresee the consequences that may arise from a certain act"; „a norm is predictable only when it is drafted with sufficient precision, in such a way as to allow any person - who, if necessary, can call on specialist advice - to correct his/her conduct"; „in particular, a norm is predictable when it offers a certain guarantee against arbitrary interferences of public power".

The main tasks of tailing were to study and establish the behaviour and preoccupation of the monitored elements in different places or environments, as well as the activity carried out at the buildings or places under surveillance, discovering the methods, procedures and means used by the targets to prepare and commit criminal acts, establishing a personal or impersonal connection, detecting tailing or evading tracking, selecting between directly contacted persons, of the connections or visitors and filtering them for identification, establishing the addresses visited by the targets. Tailing consisted in documenting the activity carried out by the monitored objectives or at the watched ones, through secret photography and filming, the drawing up of reports on performance of preliminary acts, the discovery, preservation and obtaining of evidence related to the preparation or commission of crimes or resulting from their production.

Even if, in terms of content, tailing is similar and overlaps in places with the special surveillance method, in terms of authorisation and use of the obtained evidence, there are substantial differences.

First of all, the authorisation of video surveillance, its audio through photography is ordered either by the judge of rights and liberties, or in special cases, provisionally, by the prosecutor, while tailing was ordered by the commanders of the central security information units at the request of the interested information subunits. In the case of complex security actions, which must be carried out on a certain line of work with the participation of larger security forces, the measure is decided by the head of the State Security Department at the proposal of the Special Security and Investigations Unit. Tailing measure was ordered by the commander of the security units at the request of the staff within the security units and left room for arbitrariness. The procedure itself was deficient, a fact that led to many escalations/sways during the communist period and to mass surveillance of the population. The reason why special surveillance methods must be authorised based on a well-regulated framework, by magistrates who meet the criteria of objectivity, is to respect the right to privacy and prevent arbitrariness on the part of state bodies.

6 According to art. 169 CP 1969, disclosure of documents or data that constitute state secrets or other documents or data, by a person who comes to their knowledge due to his/her duties, if the act is likely to endanger state security, is punishable by imprisonment from 7 to 15 years and the prohibition of certain rights.

In addition, the surveillance measures must be exclusively secret during the period of their implementation, which is the reason why the current Criminal Procedure Code obliges the subjects of a technical surveillance mandate to be informed within no more than 10 days after the termination of the measure, regardless of how the case is resolved.

During the communist regime, the tailing was ordered for a determined period, *i.e.* continuous tailing of the objectives was ordered for a maximum duration of 5 days, the intermittent tailing for a period of up to 7 days and at operative moments for a duration of several hours. Even if the provisions of the Instructions regarding tailing and investigations work stipulated that tailing measure was ordered for a specific period, which varied from a few hours to 7 days; the maximum number of extensions of the measure was not stipulated, nor was the maximum total period.

This precarious regulation of the measure gave way to arbitrariness, the Security bodies were the ones who proposed and authorised the measure, which had a strong secret character, a fact that led to mass surveillance of the population. In addition, the measure could not be censured by a judge and there were no nullity cases that would allow the exclusion of evidence obtained in violation of the law from criminal files. During the communist period, surveillance methods were predominantly secret and were implemented by the Security bodies.

3. The evolution of the legislation since 1978 – the forms of informative-operative activity

The legislation regulating a form of surveillance methods underwent important changes in 1978, brought by means of the Instructions D00190/1987 approved in the meeting of the Management Council of the State Security Department on June 24, 1987.

In the statement of reasons, the legislator mentions that the main purpose of the instructions was to outline a new, perfected framework for the organisation and conduct of security information-operational activity.

In the process of the informative-operative activity, the security bodies had several specific methods to collect and exploit information regarding persons, facts or circumstances of interest for the security of the state. The informative-operational activity represented a continuous and complex process of search, verification and preventive exploitation of information that could be completed by starting the criminal investigation.

These specific methods, among which we mention operative surveillance and operative tailing/shadowing, are the predecessors of special surveillance methods.

3.1. Informative surveillance

One of the main means by which the security bodies could achieve their specific missions was informative tailing, which consisted in the continuous activity of searching for data and information about facts and circumstances that may be the basis for the commission of crimes or other antisocial acts under the competence of the security bodies.

The surveillance activity was carried out in all objectives and areas of interest, both among Romanian citizens and among foreign citizens.

The measure of informative surveillance offered no guarantee against arbitrariness. First of all, it was regulated by secondary legislation, adopted by the Management Council of the State Security Department, having a strictly secret character, and the persons, either Romanian or foreign citizens, did not have the possibility of knowing the content of the instructions and implicitly also under what conditions they could be monitored.

In addition, the provisions of the instructions did not provide certain objective conditions that must be met for a person to be the object of the informative tailing measure, so that the security bodies were the only ones to assess who was necessary to be monitored. Even if the surveillance measure implied a high interference in the right to privacy of the people, the approval and implementation of this measure was the prerogative of the security bodies only, which could survey anyone without the existence of a real filter. The provisions of the Instructions no. D – 0019/1987 which regulated the informative surveillance did not regulate a procedure for authorising the measure, or a way of implementing it.

The materials resulting from the execution of the operative surveillance were preserved in a problem or objective file. Within 30 days, the security bodies, with the approval of the hierarchical superiors, exploited the

resulting materials by taking preventive measures, starting the criminal investigation, continuing to clarify the information, or classifying and destroying the materials.

3.2. Informative tailing

A form of informative-operative activity, an extra-procedural measure from which special surveillance methods originate, is informative tailing. Although it was of extrajudicial in nature, informative tailing was started on the persons about whom information had been obtained that they would prepare, commit or have committed crimes under the jurisdiction of the security bodies, as well as on the facts, criminalised by law as crimes against the security of the state. The infralegal provisions detailed the situations in which informative tailing could be carried out, *i.e.*, when there was information from which there were clear indications that certain persons would prepare or commit crimes within the competence of the security bodies, in situations where there was definite information that certain persons were committing crimes under the jurisdiction of security bodies and when facts criminalized by law were criminalised as crimes against state security.

Informative tailing was a measure authorised and implemented by the security bodies through which the information regarding the preparation or commission of crimes under the jurisdiction of the security bodies was verified. The purpose of informative tailing was to prevent the implementation of plans of hostile actions, and in the process of informative tailing it was forbidden to cause a person to commit or continue to commit a criminal act.

Following the informative tailing activity, a surveillance file was opened containing the plan of measures, and which was approved by the superiors of the central security units, or by their deputies, as well as by the superiors of the military counter-intelligence services. The informative tailing files were periodically analysed, at least quarterly, following the stage of the implementation of the measures and their efficiency. Informative tailing files older than one year were analysed at the hierarchical level higher than the one that approved their opening.

There was no procedure for authorising this measure, but only the body that had the authority to authorise it, that is, the hierarchical superior of the security bodies who proposed and later implemented the measure, so there was no real filter to assess the appropriateness of the approval measure.

The informative tailing file was closed when the preventive measures reached their goal, when the court decision remained final, by recruiting the person who was the object of the measure, or by reporting to other bodies, when the resulting issues did not concern the security of the state.

4. Regulation of special surveillance methods by Law no. 281/2003

During 2003, a criminal procedural reform took place, and the legislator substantially improved the Criminal Procedure Code. On this occasion, the special surveillance method of conversations or communications surveillance was regulated for the first time in section V^1.

Law no. 281/2003 introduced a new section „audio or video wire tapping" in the Criminal Procedure Code from 1968 with six new articles that regulated the procedure by which special surveillance methods were authorised and implemented.

From the terminology of the section „wiretapping and audio or video recordings", it can be seen that the legislator regulated only two special methods of surveillance, namely the wire tapping and the audio or video recording of conversations or communications. According to the previously mentioned legal provisions, wiretapping and recordings on magnetic tape or on any other medium would be carried out with the reasoned authorisation of the court, at the request of the prosecutor, if there are data or solid indications regarding the preparation or commission of a crime for which the criminal investigation is carried out *ex officio*, and wiretapping and recording are necessary to find out the truth. From the analysis of the law text, several conditions can be identified for the authorisation of special surveillance methods. First of all, the case had to concern a crime for which the criminal investigation is carried out *ex officio*, which can be found in the enumeration in the second sentence of the article, or be a serious crime that cannot be discovered, or which is committed by means of telephone communication or other means of telecommunications.

The legislator's option to allow the use of special surveillance methods only in the case of crimes for which the criminal prosecution is carried out *ex officio*, is not immune to any criticism, since serious crimes affecting

important social values can be identified in the Criminal Code, for which prosecution is carried out upon prior complaint, for example rape.

Secondly, the legislator leaves open the list of crimes for which special surveillance methods can be authorised, since after listing the crimes for which special surveillance methods can be authorised, respectively *the crimes against national security provided for by the Criminal Code and other special laws, such as and in the case of the crimes of drug trafficking, arms trafficking, human trafficking, acts of terrorism, money laundering, forgery of coins or other values, in the case of crimes provided for by Law no. 78/2000 for the prevention, discovery and sanctioning of acts of corruption*, the legislator provides that special surveillance methods can be authorised in the case of serious crimes, without regulating an objective criterion, by reference to which their seriousness can be established.

Consequently, in the absence of the regulation of a criterion by reference to which the judicial bodies can establish the seriousness of a crime, the legislator left room for the arbitrariness and different interpretation of the seriousness by the judicial bodies.

I consider much more inspired the legislator's option in the new Criminal Procedure Code which conditions the authorisation of special surveillance methods upon carrying out the criminal investigation for a crime with a penalty limit of 5 years or more, without having relevance if the criminal investigation is carried out *ex officio* or at prior complaint.

Another condition provided by the legislator for the authorisation of special surveillance methods was that such measures should be necessary to find out the truth, when establishing the factual situation or identifying the perpetrator cannot be achieved based on other evidence. In order to approve the use of the evidentiary procedure of special surveillance methods in the criminal trial, it was necessary that, on the one hand, it leaded to the discovery of the truth, and on the other hand, the discovery of the truth, which requires the establishment of the factual situation and the identification of the perpetrator, could not be based on other evidence. Practically, in this condition, two characteristics the special surveillance methods for authorisation must fulfil are regulated, respectively the necessary character for finding out the truth and the subsidiary character, in the sense that finding out the truth in the criminal case can only be achieved by using special methods of surveillance, it being not possible to administer other means of proof that would satisfy this desire.

The subsidiarity condition is firmly regulated by Law no. 281/2003, in the sense that it has an absolute character, finding out the truth in question must be possible only by using special surveillance methods and not other evidentiary procedures, unlike the new Criminal Procedure Code which regulates this condition more loosely. In the new Criminal Procedure Code, special surveillance methods can be approved even if finding out the truth can also be achieved through the administration of other non-special means of evidence, if obtaining the evidence would entail special difficulties that would prejudice the investigation or there is a danger to the safety of persons or valuables.

The necessity character is regulated by art. 91^1 of Law no. 281/2003 and stated that wiretapping and audio or video recordings could only be authorised if they are required to find out the truth. Law no. 281/2003 implicitly regulated the special nature of interceptions and audio or video recordings, unlike the current Criminal Code, which explicitly regulates in the title of the chapter the special nature of such measures. The special character lies in the fact that these evidentiary procedures, which involve a more pronounced interference with the right to privacy of individuals, have a subsidiary character compared to the other evidentiary procedures regulated by the Criminal Procedure Code and can only be used in exceptional situations, expressly regulated by the legislator.

From a procedural point of view, wiretapping and audio or video recordings of communications are carried out in the criminal proceedings only with the reasoned authorisation of the court at the request of the prosecutor. The request could only be made by the prosecutor, not by the criminal investigation bodies, within any prosecution unit. On the other hand, within the court, only the president of the court had the authority to authorise the use of such evidentiary procedures.

The magistrate who authorised the measure had to have a double capacity, that is one judicial, of judge, and one administrative, of President of the court. The legislator's option to condition the competence to authorise an evidentiary procedure in the criminal proceedings of an administrative nature, namely to the court president, appears to be bizarre. I believe that the measure should be authorised by a magistrate who has the capacity of a judge and not the position of President of the court, as an administrative position should not be relevant in legal proceedings.

According to the law on the organisation of justice, each court is led by a president who exercises managerial powers for the purpose of efficiently organising court activity, therefore the position of president of the court is an administrative function, so the legislator's option to assign a legal character to an administrative position is unfounded.

In addition, given the secret nature of special surveillance methods, I believe it is inappropriate for all special surveillance measures under the jurisdiction of a court to be authorised by a single judge. In addition, in order to leave no room for arbitrariness, the request for authorisation of special surveillance methods needs to be distributed randomly, and if the competence to resolve such a request belongs only to the President of the court, there cannot be a random distribution.

The evidentiary procedure could be approved for a period of up to 30 days, with the possibility of extending the measure, each extension not exceeding 30 days. The maximum duration of the recordings could not exceed 4 months in the criminal case. The term was a substantial one, as the time limitation of the measure protects the right to privacy, a pre-existing right to the criminal proceedings and independent of it. In contrast, the current Criminal Procedure Code allows the authorisation of special surveillance methods in a criminal case for a maximum duration of 6 months, with the exception of video, audio or photographic surveillance in private spaces, which cannot exceed 120 days.

5. The use of special surveillance methods in the criminal proceedings

In Romania, special surveillance or investigation methods are evidentiary procedures that can be used in cases involving serious crimes. Special methods of surveillance are vital tools in criminal trials, with the help of which investigative bodies fulfil their obligation to ensure the discovery of the truth.

Surveillance by technical means in the criminal proceedings has seen an evolution from both a legislative and an operational point of view. Currently, a large part of criminal activity is carried out or planned through electronic means, communication being carried out through encrypted messages, on the dark net, social media, so it is normal for investigators to have at their disposal adequate tools to discover and prove such crimes. The use of surveillance in the criminal proceedings in order to obtain evidence takes the form of a complex evidentiary procedure, which can only be authorised in a procedural framework, when the conditions stipulated by law are met.

These evidentiary procedures are useful for finding out the truth, but they involve a high interference with the right to privacy, so it is necessary to have a balance between the proper conduct of the criminal investigation and the limitation brought to the right to privacy. The evidentiary procedure of the interception of communications has a special and secret character, which implies a deep intrusion into the right to privacy, so the legislator has regulated several guarantees from which the person under surveillance benefits in order to respect the right to a fair trial and to limit arbitrariness in the interferences to the right to privacy.

5.1. The need for guarantees

In the last decade, international concerns have been expressed about the limitation of the right to privacy, through the surveillance of individuals by state agents or even by private entities. The first concerns about mass surveillance arose in the U.S. after the publication of the Patriot Act[7] in 2001, which allows investigators to use tools in the fight against terrorism that imply a high interference with the right to privacy.

These concerns about mass surveillance were amplified by the disclosure of secret NSA documents in 2013 by Eduard Snow,[8] which attested to the mass surveillance of citizens. The documents show that during the period 2001-2006, President George W. Bush authorised the NSA through a secret decree to collect the metadata provided by all mobile phones, as well as the emails available on nine of the largest servers. Seven years later, the United States Court of Appeals for The Ninth Circuit ruled in *United States v. Moalin*[9] case that the NSA's warrantless bulk metadata collection program was unconstitutional.

In Great Britain, until 1980 the interception of communications was authorised by the Home Secretary, without a legal framework regulating a procedure on the basis of which such measures would be authorised. In

[7] *https://www.forbes.com/sites/forbestechcouncil/2020/09/25/the-state-of-mass-surveillance/?sh=1ccd6285b62d*.
[8] *https://www.crf-usa.org/images/pdf/gates/snowden_nsa.pdf*.
[9] *https://www.aclu.org/sites/all/libraries/pdf.js/web/viewer.html?file=https%3A%2F%2Fwww.aclu.org%2Fsites%2Fdefault%2Ffiles%2Ffield_document%2F85-1._opinion_9.2.20.pdf#page=1&zoom=auto,-12,798.*

Malone v. UK[10] case, ECtHR found that this procedure was not compatible with the right to privacy regulated by art. 8 ECHR.

In that case, Mr. Malone, an antiques dealer, was on trial from June to August 1978, accused of concealing several stolen goods. He complained that his right to privacy was violated, as his telephone conversations were wiretapped based on a warrant issued by the Home Secretary.

In the reasoning of the decision, the Court reiterated the opinion that „the phrase in accordance with the law" does not only refer to domestic law, but refers also to the quality of the law, requiring that it be compatible with the rule of law, which is expressly mentioned in the preamble of the Convention. The phrase thus implies – and this follows from the object and purpose of art. 8 – that there must be a measure of legal protection in domestic law against arbitrary interference with the right to privacy on part of public authorities, especially when a power of the executive is exercised in secret, the risks of arbitrariness are obvious. Undoubtedly, in terms of foreseeability, they cannot be exactly the same in the special context of the interception of communications for the purposes of police investigations as they are when the object of the relevant law is to place restrictions on the conduct of persons. In particular, the requirement of foreseeability cannot mean that a person should be able to foresee when the authorities are likely to intercept his/her communications so that he/she can adapt his/her behaviour accordingly. However, the law must be clear enough in its terms to give citizens adequate indication of the circumstances in which and the conditions under which public authorities are empowered to resort to this secrecy. (...) Since the practical implementation of secret communications surveillance measures is not subject to the control of the individuals concerned or the general public, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of unfettered power. Consequently, the law must indicate with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise, having regard to the legitimate purpose of the measure in question, to provide the individual with adequate protection against arbitrary interference.

Following the decision of ECtHR in 1885 the Communications Act was passed, which regulates a procedure for interceptions a person's conversations. However, the law proved not to be infallible, and in the case of *Khan vs. UK*[11], ECtHR ruled that the procedure under which the interception of conversations was authorised did not provide sufficient guarantees against the arbitrariness of state bodies.

In the reasoning of the decision, the Court held that it is not disputed that the surveillance carried out by the police in this case constituted an interference with the applicant's rights under art. 8 § 1 ECHR. The main issue is whether this interference was justified under art. 8 § 2, specifically whether it was „in accordance with law" and „necessary in a democratic society" for one of the purposes listed in that paragraph. The Court recalls, together with the Commission in the Govell case (see para. 61 and 62 of the report cited above), that the phrase „in accordance with the law" does not only require compliance with domestic law, but also refers to the quality of that law, requiring that it must be compatible with the rule of law. In the context of covert surveillance by public authorities, in this case the police, domestic law must provide protection against arbitrary interference with an individual's right under art. 8. In addition, the law must be sufficiently clear in its terms to provide individuals with an adequate indication as to the circumstances in which and the conditions under which public authorities are entitled to resort to such covert measures. At the time of the events in this case, there was no legal system governing the use of covert listening devices, although the Police Act 1997 now provides such a legal framework. The Home Office guidance at the relevant time was neither legally binding nor directly accessible to the public.

Based on the decisions of the Strasbourg Court, the UK legislator adopted the Regulation of Investigatory Powers Act (RIPA) in 2000. Prestigious theorists[12] analysed the law, which in the first part provided for a new procedure which applied to public and private communications, in which The Home Secretary could issue a warrant if there were several reasons why the interception of conversations was necessary in a democratic society and if it was proportionate to the aim pursued.

The second part of the law regulated a procedure for three forms of surveillance. Directed surveillance was a form of covert surveillance that did not involve intrusive methods. Intrusive surveillance was a form of surveillance which involved breaking into private spaces or vehicles. The third form of surveillance was done by

[10] (1985) 7 EHRR 14 *https://data.guardint.org/en/entity/7dczy15vda9*.

[11] (2000) 31 EHRR 1016.

[12] L. Campbell, A. Ashworth, M. Redmayne, *The Criminal Process*, 5th ed., Oxford University Press, 2019, p. 92.

using undercover sources, people who built a close relationship with the target person in order to obtain information.

The authorisation of directed surveillance and the use of undercover sources was ordered by a senior police officer when there were reasonable grounds, before the forces were engaged in surveillance activities, and intrusive surveillance was authorised by the head of a police unit and only in urgent cases by a senior police officer. The Act provided for a Judicial Commissioner to review post-execution surveillance warrants issued by the police and a court to deal with any complaints about the manner in which the warrant had been issued.

The legislation saw an improvement in 2016 when the Investigatory Power Act was adopted, which provides the detailed procedure for issuing a warrant for technical surveillance, obtaining communications data, retaining communications data, interfering with technical equipment. In the first part of the law, the procedure for issuing surveillance warrants by the Home Secretary is provided, when national security is at risk, to prevent or detect a serious crime, or to protect the economic well-being of Great Britain to the extent where these interests are also relevant to national security interests. In the second part of the law, the procedure for issuing a warrant by a Judicial Commissioner was provided when the interception is necessary in a democratic state to find out the truth, and the measure is proportionate to the goal pursued.

In Italy, a country whose criminal procedural law system has the same architecture as that of Romania, the wire tapping was first regulated by the Rocco Code in 1930, being a tool at the disposal of state bodies to discover and prove the conduct of criminal activities.

Law in Italy has seen a continuous evolution, being one of the modern legislations that regulates in detail the procedure on the basis of which the interception of conversations or communications can be authorised, but also that has kept pace with technological evolution and regulates the interception of conversations conducted through applications that I use end to end encryption, through the computer capture.

The interception of communications could only be ordered if there were serious indications that certain serious crimes specifically designated by the legislator had been committed, and the measures were absolutely indispensable for the investigation.

In terms of content, two types of interception of communications are foreseen, the interception of telecommunications and the interception of conversations carried out in the ambient environment, which can also be achieved by remotely installing a computer recorder on a mobile device belonging to the person under surveillance that can activate the device's microphone and intercept communications, including when the subject is not engaged in a telephone call. The measures can be authorised by the investigating judge at the proposal of the public ministry, and in urgent cases by reasoned decree the measure can also be authorised by the prosecutor, under the condition of the subsequent validation of the investigating judge.

In the specialized literature[13], it was noted that in Italy, before this special surveillance method was explicitly regulated, there was a non-uniform judicial practice regarding the exclusion of evidence thus obtained. The first decision of this kind was in 2009, when the Court of Cassation ruled on the legality of the ordinance of the Public Ministry that approved the installation of a „Trojan horse" computer program in the personal computer of a criminal. In order to put an end to the non-unitary judicial practice, the Italian legislator regulated, through Law no. 103/2017, the method of consenting to the interception of „inter prasentes" communications by means of trojan horse-type computer programs installed in mobile electronic devices. The law provides that this special method of surveillance, called „captatore informatico", can be approved by the investigating judge only in the case of crimes of organized crime, terrorism or against the freedom of individuals, when there is evidence previously administered, and the measure is proportionate to the interference with private life. It is foreseen the possibility of the criminal investigation bodies to call on specialists for the implementation of this special surveillance method, considering the specific knowledge in the field of informatics that the specialist who implements this measure must have. All the activities carried out during the implementation of the measure must be recorded in detail in a minute, and the programs used must have the ability to ensure the integrity of the captured data and be authorised. As a result, the computer recorder, regulated in detail by Law no. 103/2017 and the Italian Code of Criminal Procedure, can be used both to intercept conversations conducted via the mobile applications Whatsapp, Telegram, Facebook messenger, and to intercept conversations conducted in directly

[13] R.B. Călin, *Vidul legislativ care generează imposibilitatea interceptării comunicațiilor purtate prin intermediul aplicațiilor mobile tip Whatsapp, Telegram. Facebook messenger*, in Caiete de drept penal no. 1/2022, Universul Juridic Publishing House.

between two or more people present in the same place, by remotely activating the microphone of the smartphone in the possession of a person participating in the discussion.

The Romanian Criminal Procedure Code does not allow the use of a „Trojan horse" computer program to intercept conversations carried out through mobile applications such as Whatsapp, Telegram, Facebook messenger, which is the only method by which communications carried through mobile applications that use encryption can be intercepted end to end. According to art. 138 para. (2) CPP, interception of communications or any type of communication means the interception, access, wiretapping, collection or recording of communications made by telephone, computer system or any other means of communication. Analyzing the legal provisions, it is found that it is allowed to intercept communications carried through mobile applications such as Whatsapp, Telegram, Facebook messenger, but it is not allowed to interfere with a computer system that runs the applications, in order to install a „Trojan horse" type of computer program. thus it is impossible to enforce a technical surveillance mandate regarding the interception of communications carried through mobile applications. In conclusion, even if the interception of communications carried through mobile applications such as Whatsapp, Telegram, Facebook messenger would be approved, this measure cannot be enforced, an impossibility generated by a legislative loophole that does not provide for the possibility of installing „Trojan horse" type computer programs.

5.2. Substantive and procedural guarantees

In the criminal proceedings, the legislator regulates an obligation for the judicial bodies, namely that of finding out the truth about the facts and circumstances of the case, as well as about the person of the suspect or the defendant. The fulfilment of this obligation is possible only by administering the entire palette of evidentiary procedures regulated by the Criminal Procedure Code.

In exceptional cases, judicial bodies can use special surveillance methods, evidentiary procedures that involve a high interference in the right to privacy of individuals. Considering the special character of these evidentiary procedures, as well as the high interference they entail, a series of guarantees have been regulated to ensure the right to a fair trial and to have a high protection against arbitrariness.

Guarantees can be divided into two categories, depending on their nature, substantive (substantial) guarantees and procedural guarantees. Substantial guarantees are those that relate to the substance of the rights protected pre-existing to the criminal proceedings, and procedural ones are those that refer to the acts and forms completed in the criminal proceedings.

5.2.1. The existence of a clear, predictable and accessible legislative framework – a substantial guarantee

The interception of communications is a special evidentiary procedure, and in order to respect the rights of the persons under surveillance and for there to be guarantees against arbitrariness on the part of the state bodies, it is necessary that the procedure on the basis of which the measure is authorised, the content of the measure and the way of execution are regulated in detail by primary legislation. The existence of a clear and predictable legislative framework is a substantial guarantee that must exist in any field that is legislated, but especially in the matter of special surveillance methods, which are implemented secretly by state bodies without public control.

In the rich jurisprudence[14], ECtHR has repeatedly stated that any interference by a public authority with the exercise of a person's right to privacy and correspondence must be „prescribed by law". This expression not only requires compliance with domestic law, but also refers to the quality of that law, requiring it to be compatible with the rule of law. In the context of secret measures of surveillance or interception of communications by public authorities, due to the lack of public control and the risk of abuse of power, domestic law must provide some protection to the individual against arbitrary interference with the right to privacy. Thus, domestic law must be sufficiently clear in its terms to provide citizens with an adequate indication of the circumstances and conditions under which public authorities are empowered to resort to any such secret measures.

For a regulatory act to be considered law in the sense of ECtHR[15], jurisprudence, the act must be clear, predictable and sufficiently accessible. A rule cannot be regarded as „law" unless it is formulated with sufficient

[14] Case *Halford v. The United Kingdom* (app. no. 20605/92), point 49.
[15] Case *Silver and others v. The United Kingdom*, 25.03.1983, points 87-89.

precision to enable the citizen to regulate his conduct: he must be able, if necessary, with adequate advice from a legal professional, to foresee the consequences on which a certain action can train them. A law conferring a discretion must indicate the scope of that discretion. However, the Court has already recognized the impossibility of achieving absolute certainty in lawmaking and the risk that the pursuit of certainty may involve excessive rigidity.

The quality of the law requires sufficient definition of its content, so that the scope can be determined. The terms and expressions used by the legislator must be sufficiently elaborated, to correspond to the legislative technical requirements specific to the legal norms.

The requirements regarding the quality of the law are higher in the field of surveillance measures, for which the Court specified[16] that in the special context of secret surveillance measures, the quality of the law does not mean that a person should be able to foresee when the authorities are likely to resort to covert surveillance to adjust their behavior accordingly. However, especially when a power conferred on the executive is exercised in secret, the risks of arbitrariness are obvious. It is therefore essential to have clear and detailed rules on the application of covert surveillance measures, especially as the technology available for use becomes increasingly sophisticated. The law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances under which the authorities are empowered to resort to any secret surveillance and data collection measures. In addition, due to the lack of public control and the risk of abuse inherent in any system of secret surveillance, the following minimum guarantees should be established in statutory law to avoid abuses: the nature, scope and duration of the possible measures, the necessary grounds for ordering them, the competent authorities to permit, carry out and supervise them, as well as the type of remedy provided for by national law.

In the Romanian procedural law system, these guarantees are regulated by the Procedure Code, which expressly provides that surveillance measures are authorised by a magistrate in the case of serious crimes, only if the evidence could not be obtained using ordinary evidentiary procedures. The legal norm expressly provides for the maximum duration of surveillance measures, as well as the fact that it is ordered only if several conditions are cumulatively met, i.e. there is a reasonable suspicion regarding the preparation or commission of a serious crime, the surveillance measure is proportional to the restriction of the right to privacy, and the evidence could not be obtained in any other way or obtaining it would involve special difficulties that would prejudice the investigation.

Regarding foreseeability, the ECtHR in its jurisprudence[17] gave an autonomous meaning to the phrase „provided by law" which assumes that, first of all, the surveillance measure must have a certain basis in domestic law. Secondly, it refers to the quality of the law in question, requiring that it be accessible to the person in question, who, in addition, must be able to foresee its consequences on him and compatible with the rule of law. The phrase thus implies, inter alia, that domestic law must be sufficiently predictable in its terms to give individuals adequate indication of the circumstances in which and the conditions under which the authorities are entitled to resort to measures affecting their rights under the Convention.

However, predictability is not absolute and is not synonymous with certainty, in the sense that it is not necessary for the person subject of surveillance to know that he/she is being monitored, in order to adapt his/her behaviour, since in this hypothesis the measure would not achieve the goal anymore.

The accessibility of the law means bringing its content to public knowledge, which is achieved through publication in the Official Gazette. In the doctrine[18], it was held that „in order for a *lato sensu* law to be effective, it must be known by its addressees; the effects of the law are produced, therefore, after it is brought to public knowledge and after its entry into force. In domestic law, the rules regarding the entry into force of normative acts are provided by art. 78 of the Constitution, as well as art. 11 of Law no. 24/2000 on legislative technical norms for the elaboration of normative acts. This takes place, depending on the category to which the normative act in question belongs, on the date of publication in the Official Gazette of Romania or on a date subsequent to publication, established either expressly by the constitutional norm or even within the respective normative act. It is against the provisions of art. 15 (2) and art. 78 of the Constitution for a law to provide in its text, for entry into force, a date prior to its publication in the Official Gazette of Romania. In this regard, the Constitutional

[16] Case *Shimovolos v. Russia*, 21.06.2011, points 68-70.

[17] Case *Fernandez Martinez v. Spain*, 12.06.2014, points 117-118.

[18] I. Predescu, M. Safta, *Principiul securităţii juridice, fundament al statului de drept repere jurisprundeţiale*, available at *https://www.ccr.ro/wp-content/uploads/2021/01/predescu.pdf.*

Court ruled, for example, through Decisions no. 7/200218 and no. 568/2005. Likewise, the Court of Justice of the European Communities has consistently ruled that, in general, the principle of legal certainty prohibits a Community measure from having effects before its publication."

Regarding the predictability and clarity of the legal provisions that regulate the interception of conversations and communications at the initiative of the secret services specialized in gathering information, we appreciate that the legislation in the field needs to be updated. The interception of conversations and communications can be authorised at the proposal of the bodies specialized in the collection of information, in certain cases expressly provided for by Law no. 51/1991 on the national security of Romania by the president of the HCCJ or by the judges designated by the president.

Bodies with powers in the field of national security can make a proposal to the general prosecutor of the Prosecutor's Office attached to the HCCJ, and if the proposal is legal and well-founded, it is forwarded to the president of the HCCJ. The proposal to the Prosecutor's Office attached to the HCCJ can be formulated by the Romanian Intelligence Service, the state body specialized in the matter of information inside the country, the Foreign Intelligence Service, the state body specialized in obtaining from abroad the data relating to national security, and the Protection and Guard Service, the state body specialized in ensuring the protection of Romanian dignitaries and foreign dignitaries during their presence in Romania, as well as in ensuring the security of their workplaces and residences, as well as the Ministry of National Defense, the Ministry Internal Affairs and the Ministry of Justice, institutions that organize their information structures with duties specific to their fields of activity.

Surveillance activities, to prevent and combat threats to national security, are available only if there are no other possibilities or there are limited possibilities for knowing, preventing or countering risks or threats to national security, and the surveillance measures are necessary and proportionate, given being the circumstances of the concrete situation.

It is noted that the legislator provided a procedure that requires the existence of two filters, in order to issue a national security warrant, which authorizes surveillance measures to obtain information to ensure the knowledge, prevention and removal of internal or external threats to national security. Initially, the proposal is analyzed by the general prosecutor of the Public Prosecutor's Office attached to the HCCJ or by the specific prosecutors appointed by him, and if, following the analysis, he considers that the proposal is legal and well-founded, it is submitted to the president of the HCCJ for a new analysis. From this point of view, the procedure for issuing the national surveillance warrant offers sufficient guarantees, given that it is issued by a magistrate of the supreme court, who is independent and autonomous.

As for the way of exploitation in the criminal proceedings of the evidence obtained from the execution of the national surveillance warrants, considering the CCR dec. no. 55/04.02.2020, we appreciate that the legislation needs to be updated.

Through the previously mentioned decision, CCR decided that the recordings obtained on the basis of national surveillance warrants cannot be used in the criminal proceedings and found that the provisions of art. 139 para. (3) final sentence CPP, which stipulates that any recordings can constitute means of evidence if they are not prohibited by law, they are constitutional to the extent that they do not concern the recordings resulting from the performance of activities specific to the collection of information that presuppose the restriction of the exercise of some fundamental human rights or freedoms carried out in compliance with the legal provisions, authorised according to Law no. 51/1991. CCR decided that the materials obtained following the execution of the national surveillance warrants cannot be used in criminal proceedings, as the legal provisions governing the challenge of the legality of the recordings resulting from the execution of the national security warrant are not clear enough and predictable.

In the reasoning of the decision[19], CCR „notes that the regulation of the possibility of conferring the quality of means of evidence on the records resulting from the specific activities of gathering information that presuppose the restriction of the exercise of some fundamental human rights or freedoms is not accompanied by a set of rules that allow the legality to be challenged them in effective conditions. By simply regulating the possibility of conferring the quality of evidence on these records, without creating the appropriate framework that would confer the possibility of contesting their legality, the legislator legislated without respecting the requirements of clarity and predictability. However, the lack of clarity and predictability of the incident normative

[19] CCR dec. no. 55/04.02.2020, p. 55-59.

framework in the matter of contesting the legality of records - means of evidence - which results from the specific activities of gathering information that presuppose the restriction of the exercise of some fundamental human rights or freedoms, used in the criminal proceedings, determines, in fact, the realization of a formal and ineffective control, with the consequence of violating the rights and fundamental freedoms provided by the Constitution. However, conferring the quality of evidence in the criminal proceedings on certain elements is intrinsically linked to the creation of the appropriate framework that gives the possibility of contesting their legality. Thus, conferring the quality of evidence in the criminal proceedings to the records resulting from the performance of the activity specific to the collection of information that presupposes the restriction of the exercise of certain rights or fundamental freedoms of man, pursuant to Law no. 51/1991, can be achieved only to the extent in which this regulation is accompanied by a clear and explicit procedure regarding the verification of the legality of this element. That being the case, the Court finds that the legislator did not regulate a clear, coherent and predictable framework applicable in the case of contesting the legality of evidence obtained according to Law no. 51/1991. Or, the lack of clarity and predictability of the procedure for contesting the legality of the administration of evidence determines its lack of efficiency with consequences in terms of respecting free access to justice and the right to a fair trial. However, the lack of clarity and predictability of the incident normative framework in the matter of contesting the legality of records - means of evidence - which results from the specific activities of gathering information that presuppose the restriction of the exercise of some fundamental human rights or freedoms, used in the criminal proceedings, determines, in fact, the realization of a formal and ineffective control, with the consequence of violating the rights and fundamental freedoms provided by the Constitution. However, conferring the quality of evidence in the criminal proceedings on certain elements is intrinsically linked to the creation of the appropriate framework that gives the possibility of contesting their legality. Thus, conferring the quality of evidence in the criminal proceedings to the records resulting from the performance of the activity specific to the collection of information that presupposes the restriction of the exercise of certain rights or fundamental freedoms of man, pursuant to Law no. 51/1991, can be achieved only to the extent in which this regulation is accompanied by a clear and explicit procedure regarding the verification of the legality of this element."

I appreciate that it is important that the records of intercepted communications obtained following the execution of the national security warrant can be used in the criminal proceedings, considering the principle of finding the truth, a cardinal principle in the criminal proceedings.

During the criminal proceedings, it is necessary to ensure the discovery of the truth regarding the facts and circumstances of the case, as well as regarding the person of the perpetrator, and for this the judicial bodies have the obligation to administer evidence to ensure the discovery of the truth. Recordings intercepted on the basis of the national surveillance warrant can reveal vital aspects for the criminal proceedings, in cases that have as their object crimes against national security or other particularly serious crimes, so it is necessary that they be used in the criminal proceedings to find out the truth, which it is only possible if they are given the status of evidence.

Currently, considering the CCR dec. no. 55/04.02.2020 the recordings intercepted on the basis of the national surveillance warrant can only form the basis of an *ex officio* notification of the criminal investigation bodies, but they cannot be given the status of evidence in the criminal proceedings.

Consequently, we appreciate that the intervention of the legislator is required in order to regulate a predictable legal framework, which would allow a serious and concrete examination in the framework of the criminal proceedings of the legality of the recordings obtained following the execution of the national security warrant.

5.2.2. Use of interceptions only in exceptional cases – substantial guarantee

In the criminal proceedings, the judicial bodies have at their disposal a variety of evidentiary procedures to find out the truth regarding the facts and circumstances of the case, as well as regarding the person of the suspect or the defendant. From the architecture of the Romanian criminal procedure, it appears that the judicial bodies must resort to common evidentiary procedures in the first instance and only in exceptional cases, when the conditions provided by the law are met, to resort to special surveillance methods. The exceptional character of the measures is a procedural guarantee against arbitrariness.

The special methods of surveillance have an exceptional character, which is generated by the high intrusion it entails in the right to privacy of individuals. By virtue of this character, special surveillance methods are subsidiary to common evidentiary procedures, in the sense that they are authorised only when they are the only way or a reasonable way to obtain the evidence necessary to find out the truth.

By virtue of their exceptional nature, special surveillance methods can only be approved in two cases, if the evidence could not be obtained in any other way or if obtaining it would involve special difficulties that would prejudice the investigation or there is a danger to the safety of people or some property value.

Special surveillance methods cannot be authorised when the evidence to be obtained could also be provided in a non-intrusive way. The legislator intended for the judicial bodies to use evidentiary procedures that do not imply an interference with the right to privacy, and only if the evidence cannot be obtained in this way, the special surveillance methods should be used. However, from this rule there are two exceptions, the situation in which the evidence could be obtained in another way, but obtaining it would involve special difficulties that would prejudice the investigation, or when there is a danger to the safety of persons or some property the value. The incidence of the two exceptions is assessed in concert depending on the circumstances of the case, the simple resolution of the case does not imply the existence of special difficulties. The existence of special difficulties requires the obtaining of evidence in difficult conditions, through a sustained effort of the investigation bodies. In addition, there is an additional condition, in the sense that the special difficulties must lead to the prejudice of the investigation, respectively to the impossibility of establishing the truth.

The legislator presumed the condition of subsidiarity as fulfilled when there is a danger to the safety of persons or valuable goods. In the specialised literature[20] it was noted that „in this case, the need for technical supervision is not necessarily related to the impossibility or difficulty of obtaining evidence in another way, but to the fact that resorting to non-invasive methods involves a longer time, which generates risks to the life, bodily integrity or health of a person or in relation to the safety of valuable goods." In the situation where the evidentiary thesis that is sought to be proven is already proven, a request for the approval of special surveillance methods will not be approved.

5.2.3. Authorisation of surveillance measures for a limited period of time – substantial guarantee

In order to guarantee respect for the right to privacy, the surveillance of individuals by state agents must be limited in time. The national legal provisions provide for a time-limited character of the surveillance measures, regulating a maximum duration of their authorisation.

According to the provisions of the Criminal Procedure Code, technical surveillance measures are authorised by the rights and liberties judge for a period of 30 days, and in urgent cases by the prosecutor for a period of 48 hours. The measures can be extended, for well-justified reasons, if the conditions provided by law for taking the measures are met, for a period that cannot exceed 30 days. The total duration of technical surveillance measures regarding the same person and the same deed cannot exceed, in the same case, 6 months, with the exception of video, audio or photography surveillance measures in private spaces, the most intrusive surveillance measure, which cannot exceed 120 days.

However, the total duration of the technical surveillance measures may exceed the previously mentioned terms in a criminal case, if they do not concern the same person or the same act.

The terms provided by the law are substantial, as they limit the duration of some procedural measures and aim to protect a right or an extra-procedural interest.

The terms provided by the legislator for the maximum duration of the technical surveillance measures are reasonable ones, which do not have the ability to bring too much interference in the right to privacy of individuals. We believe that the provision of reasonable terms for limiting the infringements on the right to privacy by the state bodies represents a substantial guarantee in the criminal proceedings.

5.2.4. Authorisation of the measure by a magistrate – procedural guarantee

In Romanian legislation, surveillance measures involving an interference with the rights of individuals are authorised by a magistrate within the meaning of the ECtHR, respectively by the judge of rights and liberties during the criminal investigation phase. Given the high degree of interference, it is a procedural safeguard against

[20] M. Udroiu (coord.), *Codul de procedură penală, Comentariu pe articole*, 3rd ed., C.H. Beck Publishing House, Bucharest, 2020, p. 946.

arbitrariness that special surveillance methods are not authorised by investigative bodies, but by a judicial body that is independent of the executive branch and that does not participate in the criminal investigation.

According to the procedure provided by art. 140 CPP, special surveillance methods are approved only in the criminal investigation phase by the judge of rights and liberties. The evidentiary procedure of the special surveillance methods can only be administered when there is a procedural framework, after ordering the initiation of the criminal investigation in rem and at the latest until the completion of the investigations. Special surveillance methods cannot be approved during the preliminary chamber phase or during the trial.

In special cases, special surveillance methods can be approved for a period of 48 hours by the prosecutor, when there is an emergency, and obtaining the technical surveillance mandate 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. In the situation where the special surveillance methods are approved by the prosecutor, it is necessary that within no later than 24 hours from the expiration of the measure, the prosecutor should notify the judge of rights and liberties in order to confirm the measure.

Regarding the procedure for authorising the surveillance methods provided under Law no. 51/1991 on Romania's national security, it is noted that this is also approved by an independent and impartial magistrate, respectively by one of the judges appointed by the president of the HCCJ.

5.2.5. The existence of an effective appeal to challenge the authorisation or enforcement of the special surveillance measure – procedural guarantee

In the Romanian procedural system, there are several legal ways to challenge the authorisation of special surveillance methods and the manner of their execution.

The fact that the special surveillance measures are authorised by the rights and liberties judge, an independent and impartial magistrate, does not imply an absolute presumption of legality and validity, since such reasoning renders any appeal by the interested parties ineffective. Effective recourse, which would allow for an analysis of criticisms of special surveillance methods, must exist after their approval, starting from the moment when the methods are no longer secret. The establishment of an effective appeal cannot be reported at the time when the special surveillance methods are implemented, when they are characterized by the specific secrecy that these measures entail at that time, but must be reported at the procedural time that is delimited by the others by losing this character.

The Criminal Procedure Code does not expressly provide that the conclusion of the judge of rights and liberties approving the special surveillance methods can be subject to censorship in the preliminary chamber phase, but the doctrine and jurisprudence have established that the judge in the preliminary chamber phase carries out an examination including on the conclusion and materials resulting from the interception of communications. The preliminary chamber phase was regulated by the Romanian legislator as a procedure prior to the start of the trial, the purpose of which is to verify the competence and legality of the court referral, as well as to verify the legality of the administration of evidence and the execution of documents by the criminal investigation bodies.

The Constitutional Court [21]held that in the framework of the preliminary chamber procedure, to the extent that the persons provided for in art. 344 para. (2) CPP formulate requests and exceptions regarding the illegality of the evidence obtained through the technical surveillance procedure, the judge vested with the solution the case will be able to verify the fulfilment of all legal conditions relative to the technical supervision procedure.

Thus, considering that the provisions of art. 342 CPP, which regulate the subject of the preliminary chamber, refer, among other things, to the „legality of the administration of evidence", the Court held that all documents of prosecution through which the evidence on which the accusation is based was administered, in order to ensure, in this way, the guarantee of legality, independence and impartiality. The Court also held that the verification of legality, including loyalty – an intrinsic component of legality – , of the administration of evidence by the criminal investigation bodies involves the control carried out by the judge of the preliminary chamber regarding the method/conditions of obtaining and using/administering the evidence. The judge of the preliminary chamber is competent to analyze, *ex officio* or upon request, the evidence and documents, through the lens of compliance with the legal provisions, the illegalities found to be sanctioned to the extent and with the sanction allowed by law.

[21] CCR dec. no. 338/22.05.2018, published in the Official Gazette of Romania, Part I, no. 721/21.08.2018.

Regarding the measure of technical supervision, the Court observed that, according to the provisions of the criminal procedure, it is ordered by a judge of rights and liberties, exercising his control in terms of fulfilling the conditions provided for by art. 139 CPP. However, the Court held that the European court has already rejected the reasoning that leads to the conclusion that the magistrate's capacity of the one who orders and supervises the records implies, ipso facto, their legality and compliance with art. 8 ECHR, since such a reasoning renders ineffective any appeal formulated by the interested parties. Therefore, the Court concluded that, in the matter of technical surveillance measures, which constitute an interference in the private life of the persons subject to these measures, there must be a control after the approval and execution of the technical surveillance.

Considering these aspects, the Court notes that in the criminal proceedings, both the legality of the evidence and the evidentiary procedure by which the recordings were obtained can be contested. This presupposes that the judge of the case also decides on the legality of the conclusion admitting the technical supervision measure and the technical supervision mandate. The same conclusion can be drawn from those retained by the HCCJ, the Panel for resolving some legal issues in criminal matters, in dec. no. 2/08.02.2018, published in the Official Gazette of Romania, Part I, no. 307/05.04.2018.

In the HCCJ jurisprudence[22], it was held that the person subject to technical supervision measures must be able to exercise this control in order to verify the fulfillment of the conditions provided by law for taking the measure, as well as the ways of implementing the technical supervision mandate, procedure regulated by the provisions of art. 142-144 CPP. From this perspective, the *a posteriori* control in the matter must refer to the analysis of the legality of the technical surveillance measure, regardless of whether this verification is carried out within the criminal proceedings or independently of it. At the same time, CCR, in its constant jurisprudence, for example, dec. no. 338/22.05.2018, cited above, and dec. no. 802/05.12.2017, published in the Official Gazette of Romania, Part I, no. 116/06.02.2018, considering the object of the preliminary chamber procedure, emphasized that the preliminary chamber judge must carry out a thorough check, exclusively through the lens of legality, of each piece of evidence and the means by which it was administered. Consequently, the Court held that the verification of the legality and loyalty of the judicial approach in the criminal investigation phase regarding the administration of evidence excludes a formal judicial investigation. In other words, the judicial approach carried out by the preliminary chamber judge must be characterized by effectiveness, this being obtained, first of all, by creating an adequate, clear and predictable legislative framework.

As for the possibility of the judge of the preliminary chamber to censor the documents of the judge of rights and liberties and to exclude evidence administered based on his decision, the conclusion of the judge of the preliminary chamber of the HCCJ, crim. s., dec. no. 3147 of 12.12.2014, according to which the documents of the judge of rights and liberties, which ordered measures related to the evidence on which the accusation is based, are subject to control in the preliminary chamber. The same conclusion of the existence of an a posteriori control over the final conclusion by which the judge of rights and liberties pronounces on the technical surveillance measures was highlighted in the doctrine.

In the specialised literature[23], it was considered that «all acts carried out during the criminal investigation on which the accusation is based are subject to verification, regardless of the body that ordered them, authorised them or carried them out, the arguments that substantiated this conclusion doctrinal being the following: (i) according to art. 3 para. (6) CPP, the judge of the preliminary chamber pronounces on the legality of the „evidence on which the referral document is based", without the text distinguishing between the different categories of criminal investigation documents that are limited to the administration of evidence; (ii) the exercise by the judge of rights and liberties of the function of disposition on some acts and measures during the criminal prosecution is justified by the special protection granted to some particular aspects of the person's rights, regarding either his freedom or the protection of his private life, respectively those „which restrict fundamental rights and freedoms" [art. 3 para. (5) CPP]; instituted only in consideration of these limited purposes, the exercise by the judge, with regard to a specific act, of the disposition function on fundamental rights and freedoms is exclusively intended to ensure, at the time of taking a measure of a certain gravity, the protection of the values regarding freedom and the private life of persons (persons who may be other than the suspect or the defendant) and is not intended to replace any subsequent control of legality over the respective procedural act.».

[22] HCCJ, dec. no. 244/06.04.2017, published in the Official Gazette of Romania, Part I, no. 529/06.07.2017).
[23] Kuglay, in M. Udroiu (coord.), *op. cit.*, p. 909.

Consequently, in the criminal procedural law system in Romania there is a legal way that allows a subsequent control, in the preliminary chamber phase, of the judge's decision approving the special surveillance methods and of the resulting materials.

5.2.6. Informing the person under surveillance

The Criminal Procedure Code regulates the right of the person under surveillance to become aware of the limitations brought to the right to privacy, respectively of the fact that he was the subject of a technical supervision mandate. The regulation of this right is a guarantee that benefits the person who has suffered an interference with the right to privacy and is related to his right to contest the measure.

Initially, the special surveillance methods have a secret character in order to obtain evidence capable of leading to the discovery of the truth, these measures are limited in time, and after the expiration of the term, it is no longer necessary for the measures to keep their secret character.

The legislator regulated the right of persons who were subject to a technical surveillance mandate, as a protection against the arbitrariness of investigative bodies and to be able to effectively exercise the right to an effective appeal against the surveillance measure. The right of the person under surveillance to be aware of the limitations brought to the right to privacy presupposes, on the one hand, his right to be aware of the fact that he has been the subject of a technical surveillance mandate, as well as to be aware, upon request, of the content of the resulting materials following technical supervision. The information must be provided only in writing, within no more than 10 days from the termination of the surveillance measure. The term of 10 days is a substantial one, as it relates to the respect of the right to privacy.

The exercise of the right to learn about the technical surveillance measure and the content of the materials resulting from the implementation of this measure can be postponed. The prosecutor, by means of a reasoned order, may order the postponement of the information or the presentation of the supports on which the technical surveillance activities are stored or of the playback minutes, if this could lead to the disruption or jeopardy of the proper conduct of the criminal prosecution in question; jeopardizing the safety of the victim, witnesses or members of their families or would entail difficulties in the technical supervision of other persons involved in the case. The postponement can be ordered at the latest until the end of the criminal investigation or until the case is closed.

In the doctrine[24] it was noted that „the possibility of postponing the information with reasons is in accordance with the jurisprudence of the ECtHR[25], which showed that the authorities must notify the person as soon as the information can be carried out after the end of the surveillance without prejudicing the purpose for which the measure was willing." The right to information about the surveillance measure is essentially linked to the right to an effective appeal, which allows a real and serious examination of the criticisms brought about the authorisation of the measure and the way of its implementation, since to contest the surveillance measure it is necessary to know its existence and content beforehand.

CCR[26] admitted the exception of unconstitutionality and found that the legislative solution contained in the provisions of art. 145 CPP, which does not allow the legality of the measure of technical surveillance to be contested by the person concerned by it, who does not have the capacity of defendant, is unconstitutional.

In consideration of the decision, CCR dec. no. 244/06.04.2017, published in the Official Gazette no. 529/07.06.2017, it was held that the fulfilment of the state's positive obligation, in the sense of establishing an effective appeal, cannot be related to those procedural stages in the matter of technical supervision which are characterized by the specific secrecy that these measures entail at the time, but must be related to the procedural moment that is delimited from the others by the loss of this character. In other words, in the context of the procedural stages in the matter of technical supervision which are characterized by the secret specifics of these measures, the provisions of art. 140 para. (7) CPP find their justification precisely by the previously revealed character. Thus, the Court finds that the justification that intervenes in the first procedural stages and that determines the very fairness of the finality of the court decision is removed by the legislator in the procedural stage regulated by the provisions of art. 145 CPP.

[24] Bulancea, Slăvoiu în M. Udroiu (coord.), *op. cit.*, p. 1003.
[25] Case *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, 28.06.2007.
[26] CCR dec. no. 244/06.04.2017, published in the Official Gazette of Romania no. 529/06.07.2017.

Starting from the premise that, by the very ordering of the technical surveillance measures, the person under surveillance suffers an interference in the scope of his right to privacy, the Court is going to analyze to what extent the lack of *a posteriori* control of the legality of the ordering of the technical surveillance measure complies with the conditions provided by the Constitution and Convention on the Restriction of the Exercise of the Right of Access to a Court for the Purpose of Protecting a Person's Right to privacy.

The Court notes that, according to art. 21 para. (1) of the Constitution, any person can turn to justice for the defense of his rights, freedoms and legitimate interests, and, according to art. 13 ECHR, any person whose rights and freedoms recognized by this Convention have been violated has the right to effectively address a national court, even when the violation is due to persons acting in the exercise of their official duties. Considering this aspect, the Court finds that, in its jurisprudence, it ruled that, since the constitutional text does not distinguish, it follows that the free access to justice enshrined in art. 21 para. (1) of the Basic Law does not refer exclusively to the introductory action to the first court, but also to the referral to any other courts that, according to the law, have the competence to resolve the subsequent phases of the process, therefore, to the exercise of the appeals, because the defence of the rights, freedoms and legitimate interests of the persons implies, logically, and the possibility of taking action against court decisions considered to be illegal or unfounded. The Court also held that, in the exercise of its prerogatives regarding the regulation of appeals or the exemption from their exercise, the legislator must also take into account the respect of the other constitutional reference principles and texts (dec. no. 24/20.01.2016, published in the Official Gazette of Romania, Part I, no. 276/12.04.2016, para. 19, 20). On the same occasion, analyzing the relationship, as well as the way of corroborated interpretation between the constitutional provisions of art. 129 and those of art. 21, CCR ruled that, according to the provisions of art. 129 of the Constitution, „against court decisions, the interested parties and the Public Ministry can exercise appeals, under the conditions of the law".

This constitutional norm includes two articles: the first article enshrines the subjective right of any party to a process, regardless of the subject of the process, as well as the right of the Public Ministry to exercise appeals against court decisions considered illegal or unfounded; the second sentence provides that the exercise of appeals can be carried out under the conditions of the law. The first sentence expresses, in fact, in other terms the fundamental right enshrined in art. 21 of the Constitution, regarding free access to justice; this thesis therefore contains a substantial regulation. The second sentence refers to procedural rules, which cannot affect the substance of the right conferred by the first sentence. That being the case, the Court found that, regarding the conditions for exercising appeals, the legislator can regulate the deadlines for declaring them, the form in which the declaration must be made, its content, the court to which it is submitted, the jurisdiction and the manner of trial, the solutions that can be adopted and others of the same kind, as provided by art. 126 (2) of the Constitution, according to which „the jurisdiction of the courts and the court procedure are provided only by law".

However, although art. 129 of the Constitution ensures the use of appeals „under the conditions of the law", this constitutional provision does not mean that „the law" could remove the exercise of other rights or freedoms expressly enshrined in the Constitution (dec. no. 24/20.01.2016, cited above, para. 22). From the previously stated considerations, the Court finds that, in its jurisprudence, it has ruled as a matter of principle that, whenever a legitimate interest of a person is affected, this person must have the possibility to address the court with an action in which to challenge the violation thus suffered and to obtain, if appropriate, the appropriate redress, even if, in some cases, the action taken takes the form of an appeal against a court decision. The Court considers that the previously established are all the more pertinent in the situation where the safeguarding of the legitimate interest in a certain case is, in fact, confused with the protection of the exercise of a fundamental right or freedom.

The Court also observes that in the doctrine it was held that, from the point of view of its legal nature, the right of „appeal" established by art. 13 is a subjective right of a procedural nature: it guarantees, with regard to the rights and freedoms provided for by the Convention, a right of access before the domestic judge or before any other competent authority that can order the „rectification" of the litigious situation, *i.e.* the removal of the reported violation and its consequences for the owner of the violated right. Next, the Court notes that, with regard to art. 13 ECHR, the European court ruled that these provisions require that in each member state there be a mechanism that allows the person to remedy at national level any violation of a right enshrined in Convention. This provision provides for the existence of a domestic appeal before a „competent national authority" which will examine any claim based on the provisions of the Convention, but which will also provide

the appropriate remedy, even if the contracting states enjoy a certain margin of appreciation as to how to comply with the obligations imposed by this provision. The remedy must be „effective" both in terms of regulation and practical outcome. The „authority" referred to in art. 13 does not necessarily have to be a court of law. However, the attributions and procedural guarantees offered by such an authority are of particular importance to determine the effective character of the appeal offered (Judgment of 4 May 2000, pronounced in the Case *Rotaru v. Romania*, para. 67, 69).

Consequently, based on the previously mentioned decision, the intervention of the legislator would be required to regulate a procedure through which the subjects of the technical supervision can challenge the measure, even if they have no standing in that case.

6. Conclusions

Following the analysis of existing guarantees against arbitrariness and unjustified interference in the right to privacy of individuals in the matter of interception of communications in the criminal proceedings, it can be concluded that the Romanian criminal procedural law is in accordance with the ECtHR jurisprudence.

First of all, the technical surveillance measures are regulated by a legislation which meets the quality conditions, only in exceptional cases, in the situation where ordinary evidentiary procedures do not have the ability to lead to finding out the truth.

Special surveillance measures are ordered for a limited time, by an independent executive and impartial magistrate, respectively by the judge of rights and liberties, which is a guarantee against unjustified interference in the right to privacy.

Upon completion of the implementation of the special surveillance measures, the persons who were subject to them are informed about the existence of the measure and can learn about the content of the materials resulting from the surveillance. People who have been monitored / under surveillance can criticize the interference with the right to privacy and have an effective appeal to challenge them, which is a guarantee for the observance of the right to privacy and for the existence of a fair trial.

However, an update of the legislation would be necessary for its compliance with the CCR decisions. First of all, it would be necessary to legislate a clear, accessible and predictable procedural framework that would regulate a method of contesting in the process the evidence resulting from the execution of the national surveillance warrant.

Also, the criminal proceedings legislation must be improved by regulating an effective appeal for contesting the technical surveillance measure by a person who was not a defendant in the criminal proceedings.

References

- I. Neagu, M. Damaschin, *Tratat de procedură penală, partea specială*, 2nd ed., Universul Juridic Publishing House, Bucharest, 2019;
- M. Udroiu (coord.), *Codul de procedură penală, Comentariu pe articole*, 3rd ed., C.H. Beck Publishing House, Bucharest, 2020;
- T. Bene, *L'intercettazione di comunicazioni*, Caucci Publishing House, Bari, 2018;
- L. Campbell, Andrew Ashworth, Mike Redmayne, *The criminal proceedings*, 5th ed., Oxford University Press, Melbourne, 2018;
- R.B. Călin, *Vidul legislativ care generează imposibilitatea interceptării comunicaţiilor purtate prin intermediul aplicaţiilor mobile tip WhatsApp, Telegram, Facebook Messenger*, Caiete de drept penal 1/2022, Universul Juridic Publishing House;
- I. Predescu, M. Safta, *Principiul securităţii juridice, fundament al statului de drept repere jurisprundeţiale*, available at *https://www.ccr.ro/wp-content/uploads/2021/01/predescu.pdf*;
- M. Suian, *Metode speciale de supraveghere sau cercetare*, Solomon Publishing House, Bucharest, 2021.