Aspects of Comparative Law

Andrei Bacauanu

Abstract: The use of technical supervision as a probation process in the criminal trial is a topical issue, given that in recent years information and communication technologies have considerably increased the ability to collect, process and disseminate information. Technological progress results in the secrecy of correspondence being increasingly difficult to keep, and the technical means of supervision will always be one step ahead of legislation. Given the evolution of investigative methods in the criminal process, privacy protection has become a natural concern of the EU member states legislative authorities. Interference with private life is a controversial subject questioning the renunciation at privacy, as the general interest of the society, represented by the repression of crimes with a high degree of social danger, prevails over the private one.

Keywords: technical surveillance; comparative law; interception; human rights

Introduction

The notion of technical surveillance concerns the intervention of the authorized bodies in any kind of conversations or communications by telephone or other means of communication, not public, involving the idea of confidentiality between the participants.

These means of proof were appreciated as representing a modernization of the probation system in the criminal trial, underlining that the possibilities of falsifying the obtained data are counteracted by the measures for their prevention and verification. (Gradinaru, 2014)
In the context of the evolution of technology, the legislation of the world states is constantly adapting, and in order to ensure effective judicial cooperation, it tends to harmonize laws as well as to regulate unambiguous provisions.

Thus, each legislation regulates differently the conditions that need to be met for issuing a mandate to authorize the use of the electronic surveillance procedure. The applicant must generally demonstrate that the use of electronic surveillance is necessary either in the interests of national security or for the purpose of preventing or investigating crimes.

Sometimes, for the use of interception devices, the applicant must demonstrate that the offense in question falls within the category of “serious crimes”, which is variable from state to state.

Under the United Nations Convention against Transnational Organized Crime (UNCTOC)\(^1\), a serious offense is the act which, under national law, is punishable by four years of imprisonment or more. Although sovereigns regarding the regulation of the electronic surveillance procedure, the signatory states need to consider whether the regime imposed by national law on electronic surveillance is in line with the Convention.

Some states in the European Union use the special punishment maximum as a benchmark for considering a crime as “serious”, while others have drawn up a list of offenses considered “serious crimes”.

However, some offenses appear to occur almost universally. These include investigating terrorist offenses, treason and serious violent crimes such as murder or kidnapping.

Often, legislation will explicitly indicate the factors that need to be considered for issuing an intercept order. The basis for such a request will be that there are reasonable grounds for believing that a relevant offense has been, is or will be committed.

Other factors that need to be examined are the probative value of the evidence to be obtained through electronic surveillance, the opportunity of alternative probative

---

\(^1\) The United Nations Convention against Transnational Organized Crime (UNCTOC), known as the Palermo Convention, is a multilateral treaty adopted in 2000 by a resolution of the UN General Assembly and entered into force three years later.
procedures and the condition that the mandate issued is in the interest of the administration of justice.

From a criminal-law point of view, the scale of the criminal phenomenon and the evolution of technology impose a continuous adaptation of normative regulations, which requires an analysis of the various laws that have achieved greater success in combating and preventing crime. (Gradinaru, p. 364)¹

**Technical Surveillance in the Romanian Criminal Procedure Code**

In the Romanian legal system, technical surveillance measures are expressly provided by art. 139 of the Criminal procedure code.

Within the text of the law, special technical surveillance measures are listed expressly and limitatively: interception of communications and communications, access to a computer system, video, audio or photo surveillance, location or tracking by technical means and obtaining data on financial transactions of a person. (Gradinaru, 2015, p. 39)

The conditions to be met in order to allow for technical surveillance measures to be authorized by the judge of rights and freedoms are provided cumulatively by the text of art. 139 par. 1 of the Criminal Procedure Code:

“(1) there is reasonable suspicion as to the preparation or commission of an offense referred to in paragraph (2);

(2) the measure should be proportionate to the restriction of fundamental rights and freedoms, given the particularities of the case, the importance of the information or evidence to be obtained or the seriousness of the offense;

(3) the evidence could not otherwise be obtained or the obtaining thereof would entail particular difficulties which would prejudice the investigation or there is a danger to the safety of persons or property”.

Also, the offenses in respect of which technical surveillance measures may be authorized are expressly provided by the text of art. 139 par. 2 of the Criminal Procedure Code: “in the case of the offenses against national security provided by the Criminal Code and special laws, as well as in the cases of drugs or arms trafficking, human trafficking, terrorism, falsification of coins or other values,

falsification of electronic payment instruments, crimes against patrimony, blackmail, rape, kidnapping, tax evasion, in the case of corruption offenses and crimes assimilated to corruption offenses, offenses against the financial interests of the European Union, of criminal offenses committed through computer systems or electronic means of communication, or in respect of other offenses for which the law provides for imprisonment of five years or more”.

Thus, according to art. 139 and 140 of the Criminal Procedure Code, the power to order the issuance of the warrant belongs to the judge of rights and freedoms from the court which would have jurisdiction to judge the case in the first instance. However, in case of an emergency, when the delay in obtaining the authorization would seriously damage the prosecution activity, the prosecutor by motivated ordinance, may provisionally order the technical surveillance measures for a maximum of 48 hours.

As for the maximum period in which technical surveillance methods can be used by the authorities, the mandate is issued for a maximum of 30 days, period that may be extended at the request of the prosecutor, by the judge of rights and freedoms, each extension being also a maximum of 30 days. The total duration of authorized technical surveillance measures with respect to the same person and the same offense may not exceed 6 months, except for the measure of video, audio, or photo surveillance in private areas, which may not exceed 120 days. (Gradinaru, 2012, pp. 50-55)\(^1\)

It is relevant that the decision of the judge of rights and freedoms by which the issuing of the mandate or the confirmation of the prosecutor’s order is final is not susceptible to be appealed.

The majority of national court decisions reveals that the judge’s for rights and freedoms rulings trough which a measure of technical surveillance is authorized are subject to judicial control in preliminary chamber. (Gradinaru, 2016)

Given the above, we believe that would be appropriate to corroborate the provisions of special laws with those of the Criminal Procedure Code and with the relevant jurisprudence of the European Court regarding conditions permit, the magistrate empowered to give authorization, special laws still referring to prosecutors, maximum period of authorization, clearly defining the categories of offenses and persons likely to be subject of interceptions, conditions, procedures and institutions

---

categories of experts responsible for verifying the authenticity of the recordings. (Gradinaru, 2013, pp. 68-72)

Thus, given that current technology allows easy falsification of records, where there are such suspicions, at the prosecutor’s request, or the parties or ex officio, the court may order technical expertise of the recordings to verify their the authenticity and continuity. If it is found, after examination, the lack of authenticity of the records or interfering mixes in the text or removal of passages of conversation, they cannot be retained in the case and cannot be used as evidence. (Gradinaru, Checking interceptions and audio video recordings by the Court after referral, 2012)

Comparative European Union Member States Law

The possibility of intercepting the telecommunication and informatics systems is provided in the legislation of all democratic states in the European Union, but we need to take into consideration art. 8 of ECHR on private and family life, its aim being to defend the individual against any interference of the public authorities.

(Girbulet & Gradinaru, 2012, pp. 90-100)

In article 8 of the European Convention of the Human Rights, having the title “The right to respect private and family life” it is specified that: “any person has the right to respect their private and family life, their home and correspondence.” That is why it is not admitted the interference of a public authority in exerting this right but as long as this interference is specified by the law and if it represents a measure that is necessary for the public safety, national security, economic welfare of the country, the defense of order and the prevention of penal acts, as well as the protection of health or others’ rights and liberties.

As for the phone interceptions, the Court states that, even though paragraph 1 of article 8 does not mention the phone conversations, they are implied, being comprised in the notions of “private life” and “correspondence” taken into account by the text.

Therefore, it is tackled if the public prosecutors or the judges are competent in suggesting and reducing the scope of some fundamental rights outside the criminal
instruction, in the way in which CEDO defines the prosecuting charges. Although we admit the idea of the rights protection and the fundamental liberties in front of some abusive actions by instituting the fulfillment of the condition of the existence of the authorization given by the judge, we believe that, as far as the initiating of the prosecuting charges was not disposed in one cause, the judge shouldn’t get involved, because this intervention can be interpreted as a substitution of this to the official examinations, by developing other activities than those judicial, that take place within a criminal process.¹ (Gradinaru, 2011, pp. 128-135)

A compared analysis between the specifications regarding the problem discussed presents special importance, in the conditions where it is noticed, at the level of the European Union, a consolidation in the penal field, significant contributions in this respect being the principle of mutual recognition of the law decisions, the European mandate of arrest and the frame regarding the intensification of the cooperation in the field of combating terrorism and trans-border organized criminality.

Thus, from the perspective of these considerations, we will present in detail below, as an exemplification, the legal specifications in the legislation of some countries, regarding the interception of communication.

**In the German system**, listening to the conversations is allowed as long as there are enough clues to suppose that a person committed personally or as an accomplice, a serious crime (murder, genocide, rape, drug smuggling, organized crime, etc.). Also, in order to dispose of this measure, it is necessary that the supposition should be founded, a simple presumption being insufficient, and thus the investigations cannot be realized, aspect that supports the subsidiary character of the interceptions. (Gradinaru, Aspects of comparative law regarding the interceptions and audio or video recordings, 2011)²

According to the German legislation, the authorization to wiretap and record a telephone phone conversations is issued if the suspect committed a crime against peace, high treason, or crimes endangering the safety of the democratic state, or against a land and endangering the international security, or if it was committed a crime against the capacity of defense of the state. At the same time, in the German law it is disposed this measure also if some person committed a crimes against the public order or has committed some deed to instigate or be an accomplice to escape,

---

or instigation to rebel, done by a person without military quality, according to the article 16, article 19 reported to article 1, paragraph 3 from the Penal Law of the military staff.

At the same time, the Code of German penal procedure also specifies the fact that ordering the interceptions must be done by the judge of instruction or, in case of emergency, by the prosecutor, whose decision must be confirmed by the judge within 3 days, otherwise the order will be null. The order must be written and must contain the name and address of the person who will be intercepted. Actually, it must mention the type, volume and duration of the measure, which can be of maximum 3 months. This duration can be extended though, until three months at the most, if the conditions provided by article 100a of the Penal Code are met.

The authorization of the phone interception confers, the right to record the communications on magnetic tape or any other storage device. During the hearing, the Court has the possibility to opt between playing the tape or reading the transcripts. The interceptions and recordings on magnetic tape or any other type of support are done if there are founded clues regarding the preparation or committing a crime, for which the prosecution is done ex officio, and the interceptions and recording are imposed in order to find out the truth. The interception and the recording are done with the grounded authorization of the court, in the cases and conditions mentioned by the law, upon the prosecutor's request.

In the English system, the interceptions and phone recording are regulated by Communication Act, 1985. They cannot be done without a mandate given by the Home Secretary, valid for 6 months, with possibility of renewal.

The investigations are done by the police organs that, by means of authorization issued by the Home Secretary, can proceed to listening to the phone conversation in some cases especially mentioned: if the national security or the economic one of the country is in danger, or to prevent committing a crime sanctioned with prison for more than 3 years, or involving the use of violence, endangering an important financial interest, or is done by a large number of persons following the same purpose.

The judge does not have any power of control over the interceptions, they not being under their motivated authorization. The person who discovers that they are listened to can exert the attack of appeal in front of a special court, formed by lawyers appointed by the government. The court thus informed has the obligation to verify if it was respected the legal conditions of being intercepted.
In the cause Malone vs. Great Britain\(^1\), the Court noticed that the phone interceptions are not subordinated to a mandate of the Ministry of Home Affairs and underlines the contradictions contained in the jurisprudence and government interpretation. In this case, the court noticed the lack of foreseeable character and, thus, the violation of article 8, since the “English right regarding the interception of the communication is quite obscure and the subject of divergent analyses [...] and does not indicate clear enough the extension and modalities of exercise of the discretionary power of the authorities in this field.”

As per the opinion of a judge of the European Court (the opinion of judge Pettiti in the case Malone vs. The United Kingdom), the distinction between the administrative interceptions and the interceptions required by the judiciary bodies must be clearly provided by the national regulation, in order to respect art. 8 of the European Convention, thus favoring the application of the lawfulness of some interceptions in a juridical framework rather than the existence of a juridical void which permeates the arbitrary\(^2\).

**In the Belgian system**, before 1994, there was no special law to regulate the interception of phone conversations, so that the judge of instruction was not authorized to order the interception.

Beginning with the Law from 30 June 1994, the judge of instruction is allowed, for certain serious crimes, already consumed and limitedly mentioned, to authorize the listening to and recording of private conversations, and be informed about it. Also, regarding the period of time for this measure, the Code of Belgian procedure specifies the fact that the authorization can be given for a period of maximum one month, and it can be extended for one more month at a time, for six months maximum.

**In France**, on 10 July 1991 was adopted Law no. 91-646 related to the secret of the correspondence, regulating the interception of the phone conversations, conferring a legal existence to the Inter- ministry Group of Control (I.G.C.) and interceptions.

The law mentioned above authorizes two categories of interceptions, judiciary and administrative interceptions, respectively. Thus, the judiciary interceptions are, after

---


the apparition of the mentioned law, specified and regulated beginning with article 100 and until article 107 in the Code of penal procedure. This category of interceptions is ordered by the judge of instruction in the frame of a criminal or correctional business, when the necessity of gathering information is urgent and the punishment of prison specified by the law for that deed is equal to or more than 2 years. The activity is done under the authority and control of the instruction judge who ordered it. (Renault-Brahinsky, 2008, p. 331)

The decision of the instruction judge, settled for an initial duration of maximum 4 months, can be extended by repeating the whole procedure, with the same conditions of form and duration in time and must comprise all the elements to identify the relations to intercept, the crime motivating the decision to intercept and the duration of the activity.

The judge of instruction or the officer of judiciary police can ask the agents qualified in the field, to proceed to the installation of the device to intercept the phone conversations. They must write down a report for each operation to listen to and record, where it is mentioned the date and hour of beginning and end of the operation.

The information obtained, but only the “documents of information useful in finding out the truth” are transcribed in a report, and the communication in foreign languages are transcribed in French with the assistance of an authorized interpreter.

The supports to store the recordings are kept sealed. They are destroyed upon the Prosecutor Office's request, at the expiry of the duration of the public action started by the judiciary organs, an occasion to write a report of destruction.

As for the interception of the phone conversations of the persons having the profession of a lawyer, judiciary assistant or parliamentary, it cannot be done unless the instruction judge informs the Council of the Bar association where the lawyer belongs, the president of the National Assembly or the Senate, respectively.

The administrative interceptions are the phone security interceptions, authorized with extraordinary title by the Prime Minister, having as an object the research of some information of special nature, namely that regarding: “the national safety, the security of the scientific and economic potential of the country, the prevention of terrorism, criminality or organized crime, the prevention of restoration or maintenance of extremist groups.”

At the same time, in the French legislation it is specified, in article 100-6 of the Code of penal procedure, that the recordings are destroyed, by the prosecutor's diligence,
at the expiry term of prescription of the public action. In this case, the instruction judge has the monopoly in the procedure of the interceptions. No legal disposition authorizes the judiciary police to proceed to intercept in the frame of a preliminary investigation. It is noted the fact that the specification mentioned is judicious, since the solutions not to start the penal tracking are not temporary, but also not final.

**In the Italian system,** in order to impose an interception and recording of somebody’s conversations, a representative of the Public Ministry must formulate a request to a judge for preliminary investigations, when it is considered that the interceptions are compulsory for the investigation. They will be authorized in case of crimes that are punished with prison for more than 5 years, crimes related to smuggling or drug smuggling or gun smuggling, or when the phone is used to commit a crime (such as a threat on the phone).

The permit - to intercept conversations - can be obtained only for 15 days, yet it can be renewed.

The results of the interceptions are transcribed in special regime, they can be made available for the accused’ council for the defense. In case of emergency, the Public Ministry can give up the judge’s authorization for maximum 24 hours. In this situation, after the expiry of the term indicated, it is required to validate the operation by the instruction judge within 24 hours, otherwise the interceptions cannot be continued, and their results cannot be used.

The persons responsible for the fight against mafia or anti-terrorism, benefits from special power to organize interceptions, avoiding this process.

**In the Spanish system,** the intercepting of conversations is done according to the Law of penal procedure, having the name of “Ley de enjuiciamiento criminal.” According to this law, the judge is the one who can authorize to retain the private, postal and telegraphic correspondence of the investigated person, as well as to open and check it, if there are clues that by these measures could be proved some deed or important circumstances for that investigation.

Consequently, in the case Venezuela Contreras vs. Spain\(^1\), regarding the interception of a phone line in the frame of some penal investigation, the Court considered that the Spanish constitutional dispositions in the sense that “the secret of the communication and, particularly, the post, telegraphic and phone communication, is

---

guaranteed, except for when there is a judiciary disposition,” do not accomplish the condition of foreseeable character. Even though it accepted partially the support of the Government that the judge followed to observe the legal conditions (indicating in the Ordinance of that person, the crimes they were guilty of, the controlled phone line, the duration of interception, etc.), the Court drew the conclusion that the constitutional dispositions and those in the code of penal procedure were not clear enough in the moment of producing the events, and did not specify the extent and the modalities to exert the power to appreciate of the authorities in the field of interceptions.

The measure to intercept can be disposed also by the Ministry of Home Affairs or, in its absence, by the Director for State Safety, but this disposition must be communicated compulsory to a competent judge. The latter, within at most 72 hours, can confirm or revoke this resolution.

In the Danish legislation, the secret of the correspondence and communication can be violated only if there are grounded reasons to suspect that the correspondence comes or is for a person suspected for some deeds of penal nature. Breaking this fundamental right is presumed to be of essential importance for the development of the investigation and for it to have as an object a crime committed with intention and that is punished with prison for at least six years.

The interception of the conversations can be authorized thus, if there are fulfilled the conditions mentioned above. The code of Danish penal procedure, in article 782 paragraph 1, stipulates the necessity that the measure of interception should be proportional with the importance of the case.

The measures to intercept and register, according to the Danish legislation, are disposed only by judge order. This must contain, according to the Danish Code, the phone number, addresses and circumstances specific to the case, and the duration of applying the measure must not be more than 4 weeks.

In form of judge order, this duration of interception can be extended with 4 more weeks, every time when it is necessary. As in the case of the other legislations, in case of emergency, the measure can be taken by another judiciary organ. In this case, the measure can be disposed by the police, with the obligation that within 24 hours to inform the competent instance, and the latter will decide to maintain or cancel the measure, and in case it considers it necessary, it will inform the Ministry of Justice.
International Aspects Regarding Technical Surveillance Measures

In the Anglo-Saxon legislation, due to the common law, the penal procedure has a form a lot different from the one in the law on the continent.

Thus, in the United States of America, the means of proof are regulated by the law called Rules of evidence. By issuing this law, it results the fact that for the first time in the history of the United States there are laws of uniform rules regarding the proof admissibility in the procedure of the federal courts.

The legislation of the USA has a series of specifications to limit the sphere of obtaining proofs, such as the rule called exclusionary rule with application in the incipient stage of the penal investigations, and specifying that a proof, even though it could be useful to solve some case, will not be used in court unless it was obtained observing the legal procedure.

Another rule is that called the fruit of the poisonous tree specifying that, if a proof legally obtained is related to another proof that was illegally obtained, then the proof legally obtained will not be used in the trial.

The federal rules regarding the proofs (Federal Rules of Evidence) that are incidents in the American penal trial settle that there are admitted the relevant proofs. This type of proofs means the “proof that has any tendency to make the existence of any fact that determined the penal cause more or less probable than it would be without that proof”

Even though the proof is relevant, it is possible not to be taken into consideration, if its proof value leads to causing an unfair prejudice, if confusion appears among the objects of the proof or if it is confusing for the jury.

Echelon

From the point of view of the breaches of technical supervision legislation, an analysis of the Echelon interceptions system, which has raised interest both at international and at European Union level, is relevant.

Thus, on 5 July 2000, The Scientific and Technical Options Assessment program office (STOA) of the European Parliament established a commission to investigate the matter.
Echelon’s appearance raised the issue of violation of international conventions on protection against illegal intrusion into private life as well as the laws of states expressly stipulating the conditions and cases in which intrusion may occur from the point of view of technical surveillance.\(^1\)

Therefore, the system known as “Echelon” is an interception system that differs from other information systems because it possesses two characteristics that make it quite unusual:

1. the first such feature is the ability to perform quasi-total surveillance. In particular, satellite reception stations and espionage satellites enable them to intercept any telephone, fax, internet or e-mail sent by any person and inspects their content.

2. the second unusual feature of Echelon is that the system operates globally on a multi-state basis (UK, USA, Canada, Australia and New Zealand), giving greater value compared to national systems. Thus, Echelon participating States can place their interception systems at the disposal of the other, share the costs and share the resulting information.

The Temporary Committee of the European Parliament on the Echelon interception system, in its report to the European Parliament on 18 May 2001\(^2\), reveals that there is indeed a global system for intercepting communications, which works through cooperation between the United States of America, the United Kingdom, Canada, Australia and New Zealand under the UKUSA Agreement\(^3\).

It also shows that its name is ECHELON, given the evidence analyzed, and its purpose is to intercept commercial and private communications rather than military ones.

Therefore, the Council at the plenary sitting of 30 March 2000 stated that “cannot accept the creation or existence of a telecommunications interception system which

---

\(^1\) Gradinaru, (fn. 1), p. 352.


\(^3\) The United Kingdom – United States of America Agreement (UKUSA) is a multilateral agreement for cooperation in signals intelligence between Australia, Canada, New Zealand, the United Kingdom, and the United States. The alliance of intelligence operations is also known as the Five Eyes. In classification markings this is abbreviated as FVEY, with the individual countries being abbreviated as AUS, CAN, NZL, GBR, and USA, respectively.
does not respect the laws of the Member States and which violates the fundamental principles aimed at protecting human dignity”.

In this context, the European Parliament resolution on the existence of a global system for the interception of private and commercial communications (Echelon interception system) (2001/2098(INI))\(^1\), established numerous counteracting measures.

**Conclusion**

The possibility of technical surveillance by state authorities is provided for in the legislation of all the signatory states of the European Convention on Human Rights as well as of the states on other continents that benefit from advanced technology and an appropriate legislative framework to fight crime.

Increasing global crime requires that judicial bodies have reciprocal competencies in the context in which the admissibility of evidence obtained in a country, other than the one in which the criminal investigation is conducted, involves extensive discussions and may raise obstacles in the conduct of criminal proceedings.

Thus, the need for judicial co-operation in criminal matters required a continuous adaptation of legislation at European level to harmonize the fundamental differences of national criminal systems.

We note that the procedural rules developed under the aegis of the UN, the European regulations representing the creation of the European Union and the Council of Europe, as well as the national ones, show a great similarity in the procedure that is to be followed in order to legally perform this intrusion in private life, fact that attests the success of the theoretical harmonization.

**References**


\(^1\) O.J. E.C., 72 E/221, 21.3.2002.


