EUROPEAN ACADEMIC RESEARCH
Vol. II, Issue 7/ October 2014

ISSN 2286-4822
www.euacademic.org

Impact Factor: 3.1 (UIF)
DRJI Value: 5.9 (B+)

The Institute of Tapping as a Means of Seeking Evidence in Albania and Its Competition with the Human Rights and Fundamental Freedoms

IVAS KONINI
Lecturer
Department of Criminal Law, Faculty of Law
Public University of Tirana, Tirana
Albania

Abstract:

Interception of communications represents the intervention process, with the aim of adoption of text or data in a telephone or electronic communication, or any other form. Globally, privacy is defined as a perfect unknown. Whereas in Albania, the legitimate goals of interception are complex, but among them two main elements dominate, they are national security and public safety, therefore it is necessary the intervention of the State in these interceptions. The aim of this paper is on the treatment of procedural legitimacy of interceptions, as a means of seeking evidence. The legal debate about the use of tapping operations conducted is with the fact the interception to be used as evidence and it should be performed after procedural investigative body has provided evidence for an alleged offense, or will serve as the starting point for a suspected investigation. The theme is built on this basis, primarily using the analytical method and the comparative one especially with the American and the Italian system. The novelty in this paper is the need of meeting the legal process in the field of interceptions with constitutional Coverage, through the improvement of respective provisions in the Constitution of the Republic of Albania.

Key words: interception, Constitution, privacy, the State, the Criminal Procedure Code, the General Prosecutor.

Introduction

Interception of communications represents the intervention process, with the aim of adoption of text or data in a telephone or electronic communication, or any other form without the knowledge of the sender and or receiver, in order to avoid hindering the completion of the communication between the parties.

The tapping process is an early process which dates back to the development of communication exchange. European countries from the very beginning were united in the protection of the inviolability of correspondence. In the USA this is sanctioned by the Fourth Amendment to the Constitution of 1791. In Italy the discipline of telephone interceptions dates at about 1876 when the phone began to be used as a means of communication between the parties. The Code of 1913 has addressed indirectly preservation of confidentiality of communications, while more directly reflected in The Rocco Code, the fascist regime under which qualified as a hidden normative, whose administration liked the control of telephone conversations, and in particular of political opponents. Articles 226 and 339 of this code have placed significant limitations to state investigators, who can freely interfere with

In France protection of correspondence is announced by the Constitutional Assembly in the resolution dated 10 August 1789, while the Belgian constitution of 1831 there was only one article that referred only to the inviolability of secrecy of documents, while the Constitution of 1994 establishes the confidentiality of correspondence and communication.

Frequent changes of fundamental provisions of various countries in terms of preservation of privacy of the individual and the inviolability of their communication by the state, directed the policy of European states towards the consolidation of a unified stance in defence of these rights. So on November 4,

1950, was signed the Rome Convention for the Protection of Human Rights and Fundamental Freedoms.

This Convention in its Article 8 establishes the right to respect for private life, family and individual Correspondence without any hindrance from the public authorities, with the exception of restrictions established by law that is necessary in a democratic society in the interests national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. In essence, this provision has the protection of the individual from authoritarian actions of the state, and one of which is of particular importance Correspondence respecting the person, in order to protect the confidentiality of private communications.

Privacy competing with tapping

Globally, privacy is defined as a perfect unknown. Even the Strasbourg Court in its practice has been very prudent in determining the boundary between privacy and legal obligation restricting it. In the Court's interpretation, it has never given an explicit and clear definition as to what privacy means, where it begins and where it ends. Accordingly the notion of privacy is broader than that of privacy and cannot be limited "to a" narrow circle "in which the individual may live his own personal life of his own choosing, and to exclude everything that came out of the notion of the narrow circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. "(1.Castello-Robertskundër joined Kingdom, 25 March 1993)

Although Article 8 of the Convention provides as a fundamental right of human freedoms protection of Correspondence, the Strasbourg Court has interpreted this as a right that relates to continuous and uncensored

communications between individuals. Although the term correspondence seemingly presented as a simple exchange of submission and receipt of materials through delivery, the Strasbourg Court has held that the term includes in itself the telephone and electronic communications. (2.Klass against Germany, 6 September 1978). The Court has considered regularly technological advances in the field of communications, and has implemented changing interpretation of the word correspondence. In addition to traditional letters, for the purposes of Article 8 "correspondence" is considered the oldest forms of electronic communication such as telex, telephone conversations, including related information, such as date, duration and dialled numbers, pagers orders, electronic messages (e-mail) and information derived from the monitoring of personal internet use; Private radio communications, etc.

All restrictive legislation regarding the drafting of relevant legislation in the area of surveillance, the countries that have signed the Convention, namely refer to legal interpretation made by the Court of Article 8 thereof.

In the practice of the Court in the assessment of Article 8 of the Convention is estimated that the contents of interceptions (Correspondence) is not important, but most important are the ways or methods of surveillance. The wording of the article in this case allows analysis of questions such as:

- Interference in the communication is conducted in accordance with the law
- The goal of intervention is it legitimate, and
- This intervention is useful in a democratic society

To answer these questions it is important that member states that have accepted and signed the convention and are required adapting national legislation in full compliance with the requirements of the convention. This means that the design and implementation of the legislation in terms of freedoms and human rights, in respect of correspondence, is crucial to the

process of legality of tapping. The Convention itself requires the State to undertake steps to guarantee individual rights, from criminal and illegal activities of other individuals.

However the process of legitimisation of state intervention in the area of surveillance is closely related to the legitimacy of intervention and whether it is just. Article 8 of the Convention, in paragraph 2 stipulates clearly that a public authority cannot interfere in the exercise of this right except when it is in accordance with law and when in a democratic society this measure is necessary for national security, public safety, economic well-being of the country, for the protection of public order or for the prevention of crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

In a quick review of this provision we note the legitimate goals of interception are complex, but among them are two main elements dominate, they are national security and public safety. Both of these goals are closely related to each other and are the primary object of the activity of state bodies in the field of intelligence, which guarantee these rights.

National security has to do with criminal activity and hostile of various elements against the state, internal or external forces, which seek to overthrow the constitutional order, take power by force and overthrow the democratic system or takeover of territorial boundaries of a state.

Public Safety is concerned with the prevention of terrorist acts, as well as the prevention of crime and unrest in public and private environments, life assurance of citizens from elements that cause these phenomena and resulting actions preventing the destruction of property and peace of citizen.

As per above, besides protection of confidentiality of communications, state intervention in the interceptions of communications needs to be proportionate. Such intervention should be based entirely on a legal platform, which enables an individual to create a safe and confidential communication on

the one hand and, on the other hand the state to use the interception of communications as a means of ensuring efficient evidence for prevention of the consequences, in the process of investigation and discovery of unconstitutional activity, criminal and malicious, suspicious activities to national and public security. Protection of freedom and secrecy of communication has its foundation in the Constitution of that country. So the Constitution of Italy in its Article 15, states that "freedom and privacy of Correspondence and any other form of communication is guaranteed. Limitation of them can be done only by an act motivated by a judicial authority with the guarantees established by law ".

As the law provides the establishment of equilibrium between fundamental interests, where the key word of the discussion should be balance between the law and its limitations. The concept of limitation comes naturally to the concept of law. Each right arises limited, while in a system of civil coexistence, rights must be harmonized with the needs of one of the society. This is the essence of the matter in the sphere of building legislation in the area of surveillance, as should establish a fair balance between the needs of society and the right to limit individual freedom and privacy of correspondence. But in any case the scope of wiretapping legislation should be built on the basis of certain principles uniquely embraced and subject to the social conditions of different countries in particular. Not every public body in the territory of a State may carry interception of communications such a thing should be performed by specialized bodies, which national law has authorised. In any case, the law establishes procedures for the public organs authorised to carry out such procedure, but also that the law imposes obligations on persons committing such an act.

Basic principles for tapping

In the Republic of Albania special provisions operate in the field of communications interceptions and specifically organic law "for interception of telecommunications" and the relevant provisions of the Criminal Procedure Code, Section IV, "Interception on conversations or communication." In the interception of telecommunications law clearly defined the basic principles on which the authorization being issued interception of communications that are:

- Respect for human rights and fundamental freedoms, what I have referred extensively above.
- The necessity and proportionality. Necessity is connected with the necessity of interception of communications by state authorities, for achieving a legitimate aim, provided that this is the only option for achieving the legitimate aim or if there are other options, tapping could be less prejudice the rights and fundamental freedoms.

  Proportionality is a fundamental principle in the process of balancing interceptions. This principle has in its foundation, to allow those interceptions, which in relation to privacy and freedom of thought and expression, threaten the foundations of a democratic society. Any decision on tapping should take into consideration the balance of the damage caused and the freedom of individual rights and other competing interests. Confidentiality and Objectivity. Safeguarding the confidentiality of the interception takes special importance in the whole process of tapping and has a double meaning; on the one hand secret interception serves to confidentiality of the ultimate purpose of the investigation conducted, based on the information provided through surveillance. Flow of this information can serve for the failure of the preliminary investigation

on the harmonization of the data obtained through the interception, the other facts and circumstances relating to the offense provided for in law and criminal procedure. On the other hand, even if tapping does not realize the original purpose, revealing a secret can bring irreparable consequences in relation to privacy and family life of the person tapped.

- Objectivity relates to the prompt realization and in full compliance with applicable legislation interception operations, collection, transcription and preparation of the final report of the data collected in a honest and objective manner, without deformities that can change the core purpose in favour or against the intercepted subject.

Tapping legitimacy and procedures

It is important to treat the legitimacy from the procedural standpoint, of subjects, in requiring and allowing interception operations.

The powers of surveillance procedures are performed separately for interceptions are related to national security and the fight against terrorism and organized crime and in addition in order to perform the preliminary investigation as tool to be used as evidence for crimes, envisaged by the Criminal Code, developed by the prosecutor or judicial police officer. Regarding the first category of interceptions, the legislation imposes exclusively intelligence bodies of the country, in particular the National Intelligence Service, along with intelligent services at the ministry of interior and ministry of defence. At the National Intelligence Service there is a section which conducts technical processes through eavesdropping devices via telecommunications equipment, on behalf of state informative institutions.

The equipment is placed at their disposal which is considered as "core electronic command", under the administration of the office of the General Prosecutor, which makes possible the desired and authorised interception. The results of the surveillance are made known only to the head of the state institution that has requested information interception. The head of the institution is required to report to the General Prosecutor the results of the process of interception and its result. The results of interception constitute state secret and their use outside the authorized original destination gives cause for criminal liability under applicable criminal law.

Although this category of interceptions the law authorizes the heads of intelligence institutions for their implementation, the process goes through mandatory authorization issued only by the Office of the General Prosecutor. the General Prosecutor, or in his absence the prosecutor is authorised, after proving the legitimacy of the entities that make the request and evaluates the purpose of conducting interception, issues a warrant for the interception of telecommunications through telecommunication equipment. The warrant issued cannot run longer than three months, and if needed in such a case, a new request should be filed according to the same procedures above, to provide a further three month period.

The importance of tapping process in order to achieve its aim is extraordinary, as well as it is the harm from information flow. To this end the legislator has placed under total safety controls the General Prosecutor throughout the process, and the changes made to the relevant law, in the case of electronic surveillance even with a court decision, the technical processes of interception of communications will be conducted in the premises of General Prosecutor's Office. When the data collected are used to favour particular purpose or do not serve the purpose for which they are intended, they are destroyed. In case it is considered that these data can be used in favour of

protection of life and public safety, at the request of the head of the institution that has collected the data, within 72 hours of the General Prosecutor may order the preservation of these records.

With regard to the classification of interceptions for the needs of a preliminary investigation process, it is initiated by the prosecutor of the case. The prosecutor makes a request to the competent court for the validation of that request, which in turn makes the validation with motivated reasoning. In the case of wiretapping motivated reasoning will be considered explicitly all permissions allowed by law, which means that this process is necessary to continue the investigation started and there is sufficient evidence to prove the charge. In case of need for infiltration during tapping, such action is authorized in writing by the prosecutor of the case.

In case of emergency needs for performing a tapping and when there is reasonable grounds that the delay may damage the investigation, the prosecutor orders in writing for the interception no later than 24 hours from the issuance of the order for conducting surveillance, and submits the order to the court for approval of a validation request for such action. The court is to decide either on the validity or invalidity of the order of the Prosecutor within 48 hours. In case of the invalidity if this order it prohibits the tapping and results gathered up to that point are not valid and as such do not count as evidence.
At the end of the process, the results of surveillance are deposited in the appropriate folder and used as evidence in the preliminary inquiry. The criminal procedural law provides in full the conditions and means on how to develop the interceptions.

With regard to obtain evidence, tapping is classified into two categories:

- Interception of telephone conversations or communications and other forms of communication such as electronic communications, mail and any other form

of written communication or verbal between two or more persons,

- Surveillance, which means secret wiretaps photographic, film or video, as well as devices used to locate people.

In each case the criminal procedural law has set limits allowing interception depending on the offense being investigated. Thus crimes committed intentionally that provide for imprisonment of not less than 7 years maximum, and offenses of insult and threat by means of telecommunications of any kind, the prosecutor's request for surveillance is considered legal. Setting the above limit also includes surveillance in private, while tapping procedure is the same, but in public places is allowed only for offenses committed intentionally, for which the sentence to imprisonment not less, to a maximum of his 2 years.

The intercepted communications are recorded and minutes are kept, in which the transcription of the intercepted communication is included.

The use of data obtained by tapping as evidence.

The abovementioned proceedings have an ultimate single purpose, to obtain evidence in a criminal trial. Criminal procedural doctrine consists in determining the interception of communication through information flow of telematics as a means of seeking evidence, but tapping by itself cannot be considered as proof. The data collected by tapping can only be used in order to fulfil the requirements of Section 221 of the Criminal Procedure Code, which clearly defines the limits of interception for offenses that can be intercepted. Any evidence taken by tapping in violation of the law cannot be used and its invalidity can be requested at any time of the proceeding. All interceptions, even those taken individually by a person or an official person, should comply with the law. According to the

Criminal Code, the conduct of illegal tapping beyond the provisions of law, is considered a criminal offense and punishable by a fine or up to two years in prison, as otherwise actions constitute improper interference with privacy and personal secrecy dissemination.

The legal debate about the use of tapping operations conducted is with the fact the interception to be used as evidence and it should be performed after procedural investigative body has provided evidence for an alleged offense, or will serve as the starting point for a suspected investigation. Despite the different opinions expressed on this, Article 222/1 of the Criminal Procedure Code clearly defines that "… the court authorizes interception with a motivated decision to the extent provided by law, *when it is necessary to continue the investigation started and when there is sufficient evidence to prove the charge*. .....". This disposition clearly states that the process of tapping cannot start without the existence of facts and evidence on the alleged offense. The use of tapping as evidence, in reality is additional proof of evidence attached to the primary investigation and may further serve for the detection of other persons involved in the criminal investigation.

The jurisprudence in the area of interceptions, qualifies the extraction of a "motivated decision" by the court a crucial point is extraction of "motivated decision", based on a request from the authorized body for this purpose. It is as if the court (judge) assigned for this purpose should examine the case on its merits, when criminal procedure does not permit such a thing, as a decision of guilt or innocence is issued by a panel following a legal process. Then who will be the criteria that the application called "motivated". In these conditions there are no postulates to indicate the phenomenon, but it certainly would be subjective elements associated with assessment of facts presented by the prosecutor, social threat of the wrongdoing, and above all the conviction of the judge deciding that the

implementation of the procedure will affect the solution of the case with a guilty conviction or innocence of the suspected person under investigation.

Again, there is legal interpretation debate with regard to the Criminal Procedure Code provisions regarding the use of evidence obtained through tapping, in reference to Article 151 of the Penal Procedure Code. Point 4 of this Article establishes the obligation to inadmissibility of evidence obtained in violation of the prohibitions provided by law. Meanwhile, point 3 of this article, determines the possibility of using evidence taken from the court not regulated by law, provided that two conditions are met; *firstly,* if it helps to prove the facts and, *secondly*, if the freedom of will of the person, so that means that the person under investigation needs to give consent. Hence here we must distinguish between the terms "evidence in violation of legal prohibitions" with "evidence not regulated by law", as not every piece of evidence not regulated by law may be prohibited by law. In case of application of law "On the prevention and fight against trafficking of narcotic drugs or psychotropic" an undercover person authorised by law, can be assigned to perform "simulated purchase" of narcotics. During this operation undercover persons performing filming and photography, although do not have proper authorization for tapping, the evidence obtained should be admitted as evidence in accordance with the above interpretation in reference to Article 151 of the Criminal Procedure Code.

Means of evidence of electronic communications in the United States and assistance to foreign authorities.

In the USA the information, with regard to the results of tapping of electronic communications by law enforcement organs, the information can be secured in two ways, through stored information and online communication.

Stored information represents data about the subscriber, email or voice messages previously sent and that are preserved in the respective operator's server. On line communication is taken in real time, and it is obtained through the interception of communications technology.

In order to determine the level of secrecy, the burden of proof is with the state to provide such data. In this context, the deeper the privacy of the individual affected, the higher is the state's responsibility in providing legal burden. In case the information stored is much simpler to obtain the right information and be considered a minor violation of privacy in relation to interception in real time. Therefore competent authorities of law enforcement should be guided by the classification of information to provide. Thus the authorities should demand what in reality is needed, because the more they require the higher is the standard of proof before the American courts. If it turns that more information is required, the request can be repeated.

USA legislation allows law enforcement officials, that in urgent matter, to participate without prior authorisation, in order to obtain information directly from an Internet service operator. For this purpose urgent matters shall be deemed the abduction of a person and their communication with friends and family through an e-mail account, or communications of terrorists through an e-mail where an attack is predicted. In any case internet service operators must decide to deliver the available data, after they are that this data is submitted to a law enforcement agency. American law provides that the implementation of the above procedure, i.e. the collection of data via communications interception, two key conditions must be met:

- *First*, the data will be given only in emergency conditions for an "instant danger to life and severe physical damage to a person." So if a risk is not displayed, it is not real and instant, but hypothetical,

the condition of urgency for the collection of data is not met.

- *Second*, depending on the type of the risk, it is necessary to disclosure the information without delay.

As per above the legislation allows the internet service provider to take the decision, which evaluates the urgency of the matter. The service provider may reject a request to submit "voluntary" data and in such a case the possibility of providing authorization through a legal process, remains the only way to obtain data.

Data protection

Under normal conditions, each operator of internet service deletes the data from their server, regularly after 21 days to 6 months after the communication is performed. At the time of deleting data from their server, no operator can recover the data, and subsequently the data disappears definitively. In the United States there is no law to force internet service operators to maintain their server data, until destruction is authorized from a competent body. In these conditions the time of filing of the request for obtaining communication data is very important. American law does not prohibit Internet service operators to accept requests from storing communications data by foreign law enforcement bodies. Precisely for this reason many States follow the practice of requesting directly to the internet operator. However, if authorized bodies of foreign states cannot provide these data according to the above procedure, in the USA, as well as in 50 other countries worldwide, an operating unit called the Network of High Technology Crime Investigation Association 24 hours, which ensures that data 24/7, can submit their applications to all member states of the Network. If a state is not a member of this Network, may secure service through its special envoy to law enforcement at the USA Embassy in that country. Upon

receiving a request for data storage by the internet service operator, with any of the above ways, the data is stored up to 90 days, with a right to renew for another 90 days. However, during the process of electronic surveillance under the above procedure there are a number of risks, which the officials authorized to conduct tapping intervention should take into account. Cases of risk can be summarized:

- First, the subject under electronic surveillance may realize that his IP address or website is under surveillance, being informed by the service provider.
- Second, not all Internet service operators are reliable, especially at a time when the United States has no criteria for their licensing and regulations governing Internet service industry.
- Third, in terms of computer investigation, criminal organizations receive or create own internet service operators, in order to communicate away from the observations from law enforcement bodies and in terms of filing such an application, the subject is informed of the tapping, thus paving the way insecure and manipulated evidence.

Types of information protected

Three types of information can be obtained through conducting an electronic from internet service providers:

a) ***Information for the subscriber,*** which represents the lower standard of inquiry, and related data such as the name and address of the person under surveillance, as well as data on the use of the online service in a date and time assigned. In case of a request for information seizure in such a case must be proved that the collection of this information is important to the process of criminal investigation in charge of the person. Moreover the request must be filed correctly and it must determine the date, hour, minutes and seconds (possibly

time zone, e.g. "GMT") the start and end of communication, because computer users are constantly changing addresses IPs

b) ***Information on transactions,*** which represents an average standard of the investigative process. The source of information can show data in a case related to the names of the interlocutors of the person under investigation, websites visited by him, and his online activity. The purpose of using these data is relevant to an application for extension of investigation in relation to other persons who may be perpetrators or victims of crime.

Information can be obtained through the interception of transactions conducted showing connections with other people, the origin or destination of electronic messages received or sent via email the head of the "To" and "From", as well as images or other documents that may be uploaded on the website, including the date, time and file size, (but not its content).

c) ***Information on the content,*** as distinguished from that setting, represents the highest standard in a criminal investigation. Content includes information sent electronically in the form of written or voice messages, photographs or images or material attached. In such a case the national or foreign law enforcement authority must submit the request to national or foreign law enforcement authority or the judicial authorities and its underlying application must observe two essential conditions are respected "*probable cause*" and "*actuality of information*"

Possible cause is related to the possibility that evidence required can be found in text content of the internet service operator, and this data will only be used as evidence to uncover a criminal investigation. The procedure requires that the

subject of the investigation should argue that the content of the text seized, serves to the motivated purpose and show that the content of the text that will be seized relates to the offense under investigation.

Current information relates to the "updated" content about the time when it was committed. No preserved information may be requested, which belongs to the past periods and have lost their actual. With regard to the preserved data the current legislation provides that no evidence of communications can be obtained unless it is performed in more than 60-180 days. American law does not allow real-time collection of information from foreign countries, with the exception of issues that are joint investigation between the competent authorities of the two countries.

Besides containing information on the practice of tapping the USA, a significant role plays the collection of real time information without contents. This means the request conducted by law enforcement authorities for the provision of data expected to be sent via email, and is especially applicable when the subject under investigation is on the move and performs electronic communication transactions from different points of transmission. Through this operation the investigator can locate the IP address and the time of communication of the person under investigation, which leads to identify his whereabouts. Nevertheless, the United States government may refuse a request for electronic information, especially if the person under surveillance in the United States, an investigation has been launched.

Conclusions

To conclude criminal law with regards to interceptions is sufficient, while I cannot say the same for its constitutional support. All criminal law related to the necessity of the surveillance process in order to strengthen the constitutional

order, is in full competition with human rights, in reference to Article 36 of the Albanian Constitution which stipulates that "freedom and secrecy of correspondence or any other means of communication are guaranteed ". If we refer to the cited constitutional provision we will notice that the restriction of freedom and correspondence are inviolable, while the law permits such a violation in cases motivated and supported by law.

To the aid of the above conclusion, the Italian legislative practice concurrently helps, which is almost identical to the procedural standard of realization of interceptions however the Italian Constitution, in Article 15.2, states in paragraph 1, guarantees the freedom and privacy of correspondence, followed by second paragrapf as follows: "Limitation of them can only be done only a motivated act of a judicial, with the guarantees established by law". Not wanting to continue with the comments, I think such a paragraph of our Constitution is needed to fulfil the legal process of interceptions under the constitutional umbrella.

Interceptions are estimated to be an effective tool in the detection of crime in general and organized crime and international crime in particular. In view of this objective, governments of major countries, besides tapping carried out against specific individuals, increasingly are applying interceptions of strategic importance, which enable *in bloc* communications transmitted and processed through the internet, fixed and mobile telephony, SMS, MMS and any other kind of personal communication tools. These entire data cannot only be collected, but also stored for a long time, in order to be used when the need arises. But ultimately all of these have a cost, which is increasing from year to year. So just for the preservation of voice quality in interceptions last year conducted by the German government has calculated a cost of 30 million euros, while the total cost of surveillance by the Italian government for 2013 is estimated at 450 million euros.

Growing applications for tapping conversations, mainly that telephone technology is advancing towards the creation of methods to prevent interception, through encrypted communication technology. These methods consist in the creation of software that operates without the involvement of mobile operator and provider, which are installed in receiver and sender stations transmitting wave interference which make incomprehensible conversation.

BIBLIOGRAPHY

Constitution of the Republic of Albania.

Constitution of the Republic of Italy.

European Convention of Human Rights.

Interpretations of the Strasbourg Court about the concept of privacy.

Criminal Procedure Code of the Republic of Albania.

Albanian law no. 9187, date 12.02.2004 "On Amendments to the Criminal Procedure Code of the Republic of Albania".

Criminal Code of the Republic of Albania, updated.

Rocco Code, the Italian criminal code, updated April 2014.

Albanian law no. 9157 date 4.12.2003 "For the interception of telecommunications".

Guide to Mutual Legal Assistance and Extradition from USA. International Relations Office, Criminal Division, Department of Justice, USA 02/08/2011.

Code of Criminal Procedure of the Republic of Italy.

Carnuccio P, Strategies and defensive techniques in terms of interceptions, Torino 2007.

The Castello-Roberts vs. United Kingdom case, 25 March 1993.

Bartole - De Sena. Short commentary of the European Convention of Human Rights. Chapter: The means of gathering evidence.

Lovison D, The intercepts of conversations or communications, Chapter 1: The intercepts in Italian law.

Lauds M, The Practical Handbook wiretaps in criminal investigations, Milan 1986.

Avv.Comi V. La Sapienza University in Rome, interception of conversations or communications, Rome 2014

Bianku, L. The jurisprudence of the Strasbourg Court, Tirana 2005.