

DISCLAIMER: Please note that the translation of the legal text provided below is only a provisional translation and therefore it does NOT represent an official document of Republic of Albania. It is meant purely as a documentation tool and EURALIUS does not assume any liability for its contents.

Law
No. 9157, date 4.12.2003
ON INTERCEPTION OF ELECTRONIC COMMUNICATIONS
(Amended by law no. 9885, dated 030.3.2008)
(Amended by law no. 10172, dated 22.10.2009)
(Amended by law no. 116 /2012)
(Amended by law no. 69/2017)

Pursuant to Articles 78 and 83, point 1, of the Constitution, upon the proposal of a group of the Council of Ministers,

THE ASSEMBLY
OF THE REPUBLIC OF ALBANIA

DECIDED:

CHAPTER I
GENERAL PROVISIONS

Article 1
Object

(Word added by law no.69/2017, article 1)

This law establishes the procedures that shall be followed for the preventive interception of electronic communications by the state intelligence institutions established by law for the fulfilment of the duties, as well as the procedures that should be followed by the persons charged with for the conduction of interception.

Article 2
Purpose

This law aims to increase the effectiveness of the activity of intelligence state institutions for the discovery of the unconstitutional, criminal, and delinquent activity, as well as to prevent the consequences that might derive from this activity.

Article 3
Definitions

(Points 1 and 2 amended by law no.69/2017, article 2)

Point 10 added by law no.69/2017, article 2)

For the purpose of application of this law, the following definitions shall mean:

1. “Core Electronic Command” is the technical device in administration of the General Prosecution Office and of the Special Prosecution Office, which allows or forbids the interception of an electronic communication device.
2. “Object of interception” are the signals, or other forms of information, to be received or transmitted by means of electronic communication devices.
3. “Electronic communication entrepreneur” is a natural or juridical person, which provides networks of electronic communication and/or services of electronic communications pursuant to prescriptions envisaged by the legislation into force on electronic communications in the Republic of Albania.
4. “Final device” is every device in use by an intercepted person, which is connected directly or indirectly to a final point of the electronic communication network in order to realize the electronic communication.
5. “Electronic communication device” is every technical means (transmitting line, communication device, and any other device necessary to ensure the functioning of the electronic communication network) which serves for the realization of the electronic communication.
6. “Interception” is the hidden interference to capture, hear and record the content of the communication and data related with it, between the starting point and arriving point
7. “Emergent situation” is the situation when from the moment for compliance with requests laid down by this law for the submission and the approval of the written request, the interception result is damaged, entailing consequences for the national security.
8. “Intercepted persons” are individuals suspected as alleged authors of serious crimes.
9. “Communication” has the same meaning with the meaning established in paragraph 13, article 3 of the law no. 9918, dated 19.05.2008, “On electronic communications in the Republic of Albania”, amended.
10. “Competent Prosecution Office” is the General Prosecution Office or the Special Prosecution Office according to the competences provided for according to the legislation in force.

Article 4
Principles of Interception

The core principles for interception of electronic communications are the respect for freedoms and fundamental human rights, the necessity and proportionality, secrecy and objectivity in its conduction.

Article 5
Utilization of the interception outcomes

The interception outcomes, acquired on the basis of this law, do not have evidential value, except for those taken in accordance with the Criminal Code of Procedure.

CHAPTER II
PROCEDURE FOR CONDUCTION

OF INTERCEPTION

Article 6

Bodies that may require the conduction of interception

(Point 1 amended by law no.69/2017, article 3)

1. National Intelligence Service, intelligence service/ police intelligence service of the responsible ministry for the order and public safety, Ministry of Defense, Ministry of Finance, Ministry of Justice, National Bureau of Investigation, as well as any other intelligence/policy service established by law, have the right to request the interception, in order to ensure the necessary data for the fulfilment of their legal duties.
2. None of the public institutions mentioned in paragraph 1 of this article have the right to submit a request for interception for matters or activities that are not foreseen by the law as subject-matter of their informative-tracing activity.

Article 7

Interception request

(Amended by law no.69/2017, article 4)

1. The interception request, submitted by the subjects mentioned in Article 6 of this law, is prepared in two copies of which one shall be deposited before the Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, and the other one shall be held by the concerned institution.
2. The request shall contain:
 - a) the requesting institution, names and functions of the employee following the process of informative-tracing;
 - b) personal details and the address of the person subject to the process of informative-tracing or subject to tagging after, as well as the address/addresses of the areas/premises related to the electronic communication interception request;
 - c) description of electronic communications that shall be subjected to interception and, wherever appropriate, the data for the electronic communications operator who provides service to the subject who will be intercepted;
 - ç) the reasons for the interception, and the documentary support or informative material where the interception request relies;
 - d) the arguments attesting that the interception is necessary in the created situation and that the requested data cannot be assured by other means;
 - dh) the time limit within which the interception is sought.

Article 8

Granting of the right to interception

(Amended by law no.69/2017, article 5)

1. The Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, after the examination of the written interception request of the responsible Minister for order and public safety, Minister of Defense, Minister of Justice, Minister of Finance, Director of the National Intelligence Service, Director of the National Bureau of Investigation, as well as of every ministry that has under his dependency intelligence/police services established by law, approves or refuses the request for interception

of electronic communications.

The request for interception, shall be examined within 48 hours from the moment of its submission.

Article 9

Decision for Interception

(Amended by law no.69/2017, article 6)

1. The Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence the deputy chairman, takes a written decision in reply to the request for interception, which is drawn up in three copies. A copy of the decision that approves or denies the request shall be kept in the Court of Appeal against Corruption and Organized Crime, one copy shall be kept by the institution that has made the request, and the third copy shall be kept by the core electronic command of the competent Prosecution Office.

2. The request for interception, as well as all data collected by interception is confidential. Institutions involved in the decision-making process shall keep confidential every request and data collected by interception for which they have learned, unless otherwise provided by this law.

3. Interception decisions shall apply to communications via electronic communication devices within the territory of the Republic of Albania, or abroad, where there is an international agreement to which the Republic of Albania is a party.

Article 10

Content of the Decision for interception

(Letters "b" and "c" amended by law no.69/2017, article 7)

The Decision for interception shall contain these elements:

a) requesting institution;

b) responsible structure for interception within the National Intelligence Service, in the section of interception in the State Police or in the Internal Intelligence Control Service of the responsible ministry for order and public safety, in National Bureau of Investigation or, accordingly, the employees authorized by heads of requesting institutions to carry out the technical process of interception.

c) personal details and the address of the subject who is to be placed under interception; the identified areas/premises for which the electronic communication interception shall be performed, final devices used by the subject under interception for performing of the electronic communication, as well as the provider of electronic communications that offers the service;

ç) the time limit or the time limits of interception, where the data and the hour of initiation and its termination is determined.

The decision shall charge for its implementation the responsible interception structure at the National Intelligence Unit and the requesting institution.

Article 11

The change of final device

(Amended by law no.69/2017, article 8)

After the adoption of the interception decision, when it is acknowledged that final devices of the subject under interception have been added or changed, the request of

interception shall not be repeated. In this case, the state institution requesting the interception is obliged to notify in writing for the new final device the Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, who orders the respective commanding core for the change or addenda of the final device or devices which are intercepted. In this case, the time limits of interceptions shall remain unchanged.

Article 12

Interception Sector

(Amended by law no.69/2017, article 9)

1. The responsible Sector for Interceptions at the National Intelligence Service performs only the technical processes of electronic communications interceptions by means of telecommunication devices on account of state intelligence institutions, after the decision on interception has been taken in accordance with this law. The technical processes of interception, on account of the State Police and Internal Service Control in the responsible ministry for order and public safety shall be performed by their interception section, attached in the responsible Structure for Interceptions at the National Intelligence Service.

The technical process of interceptions, on account of other institutions, is performed by their authorised employed agents.

(Repealed point 2 by law 69/2017, article 9)

3. The realization of interception by the responsible Structure for Interceptions at the National Intelligence Service and the interception section of the State Police, and of Internal Service Control in the responsible ministry for order and public safety as well as by the National Bureau of Investigation is performed through systems installed for that purpose. The interception system always shall be composed of two parts, which cannot function in independent way from each other.

Article 13

Core electronic command

(Amended by law no.69/2017, article 10)

The Core electronic command is a technical device administered and installed at the General Prosecutor Office and at the Special Prosecution Office, which permits or forbids the interception of a final device. The employee of the core electronic command, after the written decision on the approval of the interception request of the Chairman of the Court of Appeal against Corruption and Organized crime, or in his absence, the deputy chairman, makes technically possible the interception process by the responsible Sector for Interceptions at National Intelligence Service, and the interception section of the State Police and of the Internal Service Control in the responsible ministry for order and public safety and by the National Bureau of Investigation, except as otherwise provided in this law.

The core electronic command employee, upon the termination of the time limit according to the decision of the Court of Appeal against Corruption and Organized Crime, automatically interrupts the interception, except when there is a request for the extension of the time limit.

Article 14

Duration of the interception decisions

(Amended by law no. 69/2017 article 11)

1. All interception decisions for the interception of electronic communications are valid for a period up to three months.

2. For every extension of this time limit, the respective state institution submits to the Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, a written and argued request together with the clearing interception material obtained so far. The Chairman or the deputy chairman according to this Article, is authorized to request explanations or additional reasons for the extension of the time limit.

3. Any extension of this time limit cannot be more than three months.

Article 15

Cognizance of the interception results

(Amended by law no. 69/2017 article 12)

1. The head of the respective state institution that has requested the interception shall know the interception results, during the time limit the interception is on-going, as well as after its termination.

2. The Chief of the Special Prosecutor Office or the General Prosecutor, or the Chief of the Prosecution Office at the Court of First Instance according to their competences, have the right to be informed by the head of the respective State institution that has requested the interception with the interception results after its completion, except when the head of the respective state institution considers that they must be informed for the results of the interception even before its termination.

Article 16

Limitations on interception

(Letter "b" amended by law no. 69/2017 article 13)

1. Persons in charge with functions or specified duties within or for the interception process as a whole or particularly are forbidden:

a) to diffuse or utilize the data acquired not in accordance with the requirements laid down by this law or other laws in force;

b) to intercept without authorization or outside the procedures setup by this law.

2. The interception process, in whole or in particular, constitutes state secret, the violation of which is punished according to the criminal legislation in force.

Article 17

Emergency situations

(Amended by law no. 69/2017 article 14)

1. For emergency situations, upon verbal request of the head of the responsible state institution, pursuant to Article 6 of this law, the Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, orders in written form for the technical realization of the interception process. The decision of the court shall be

registered immediately into the records of the core electronic command within the competent Prosecution Office and into those of the specialists of the responsible Structure for Interceptions at the National Intelligence Service, or the interception section of the State Police, of the National Bureau of Investigation and of the Internal Service Control in the responsible ministry for order and public safety. After the registration of the decision, the specialists of the responsible Structure for Interceptions at the National Intelligence Service, or the interception section of the State Police, of the National Bureau of Investigation and of the Internal Service Control in the responsible ministry for order and public safety conduct the process of interception.

2. Within 8 hours from the initiation of interception, the responsible state institution that has made the request, submits to the Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, the regular written request, which shall contain the reasons of emergent actions together with the intercepted communication after clearing them. On this basis, within 24 hours from the initiation of interception, the responsible decision to continue or to interrupt the interception shall be taken.

3. Failure to submit the written request within the time limit established in paragraph 2 of this article, shall entail the immediate interruption of the interception.

Article 18

Revocation of the interception decision

(Amended by law no. 69/2017 article 15)

If a change occurs that leads to the conclusion that the interception is no longer necessary or practical to implement, then, upon written request of the responsible state institution to the Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, to the deputy chairman, the decision is revoked.

The revocation decision shall be addressed to the responsible electronic core commands, to the requester and to the technical implementer of the interception.

CHAPTER III

SPECIAL REQUIREMENTS FOR INTERCEPTION

Article 19

Interception upon request of foreign intelligence/police services

(Amended by law no. 69/2017 article 16)

Upon request of the intelligence/police services and the approval of the Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, the responsible Structure for Interceptions at the National Intelligence Service, or the interception section of the State Police, and of the Internal Service Control at the responsible ministry for order and public safety or National Bureau of Investigation can perform, accordingly, interception pursuant to the provision of this law, on account of the foreign intelligence/policy service.

Article 20

Destruction and preservation of the interception material

(Amended by law no. 69/2017 article 17)

1. The interception material obtained by the preventive interception process of the electronic communications shall be destroyed within 10 days after the expiration of the interception time limit. The interception material shall be kept only in case there are premises that it is likely to be important for the protection of life, national security, public order or the prevention of serious crimes.

2. The head of the responsible state institution, within 3 days from the expiration of the interception time limit, submits written request to the Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, for the preservation of the interception material. The Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, shall take a decision to accept or to refuse the request within 72 hours from its submission.

3. If the request is refused, the interception material shall be destroyed within the time limit provided in point 1 of this Article, according to the procedures [modalities] established by joint instruction of the General Prosecutor, Chief of the Special Prosecution Office, responsible minister for order and public safety, Minister of Defence, Minister of Justice and of the Director of National Intelligence Service.

4. If the request for preservation of the material is accepted, the decision shall also determine the time necessary for its preservation. Upon the completion of the deadline set in the decision, the preserved material shall be destroyed in accordance with the terms and procedures provided for in this article.

Article 20/1

Right to information

(Added by law no. 69/2017 article 18)

1. The responsible state institution, within 15 days of receipt of the written request of a citizen, should inform him if any interception of electronic communication is undertaken against him/her. This information is only given after the interception has ended.

2. The citizen shall have the right to request documents on the data collected, which can be made available to him without the name of the employee who has collected them and without the data about the sources of information of the security and intelligence agencies and third parties.

3. The responsible state institution is not obliged to act according to the provisions of paragraph 1 of this Article if:

- a) the notification could jeopardize the implementation of the tasks of the institution;
- b) the information can lead to risk the safety of another person;
- c) the content of the intercepted communication constitutes state secret and may lead to harmful consequences for national security or national interests.

CHAPTER IV

ELECTRONIC COMMUNICATIONS ENTREPRENEURS

Article 21

Interception capabilities of electronic communications networks

(Point 2 amended by law no. 69/2017 article 9)

1. The electronic communication providers realize, by their own expenses, the necessary infrastructure on their electronic communication network, up to the connecting point with the core electronic command, in order to assure, within 180 from the reception of the request by the institution that administer interceptions systems, according to this law, the interception capability towards users that utilise electronic communications services provided by them.
2. The infrastructure that is realized by the electronic communication providers assuring interception capability should be technologically compliant with the devices of electronic core commands of the interception systems.
3. Electronic communication providers are obliged to provide free of charge any service in function of the interception process.
4. When electronic communication providers adopt any kind of technological change, or increase of capacity, they are obliged to cover by their own expenses the continuity of the functioning of the interception process.
5. In case of changes in the core electronic command, that impose changes in the electronic communication infrastructure of the providers, the responsible structure for the core electronic command shall notify the electronic communication entrepreneurs, at least, 180 days before this change.
6. In case of non fulfillment of the obligation pursuant to paragraph 1 of this article, Electronic Communication and Postal Authority, acts in accordance with its competencies laid down in article 18, 131 and 137 of the law no. 9918, dated 19.05.2008, "On Electronic Communications in the Republic of Albania" , amended.

Article 22

Assistance of the electronic communication providers

(Title amended by law no.69/2017, article 20)

(Amended by law no.69/2017, article 20)

1. Where the interception cannot be realized means of the interception system, the Director of the National Intelligence Service, or the responsible minister for order and public safety, accordingly, requests the assistance of every electronic communication entrepreneurs in the Republic of Albania, which are obliged to take the necessary steps.
2. In these cases, the operator is given a copy of the decision of the Chairman of the Court of Appeal against Corruption and Organized Crime, or in his absence, the deputy chairman, with an abbreviated content and without data that might impinge the intelligence-tracking process. This copy shall contain the time limit within which the operator shall provide numbers, addresses and other elements that need to be identified for the interception. When necessary, the copy of the decision shall be accompanied with an additional document, in which other technical details for the devices of the electronic communication are determined.

CHAPTER V FINAL PROVISIONS

Article 23
Interception by court decision
(Amended by law no. 69/2017 article 21)

1. The technical processes of interception of electronic communications, through telecommunication equipments, for the purpose of preliminary investigations, shall be conducted according to the articles 221 to 226 of the Criminal Procedure Code.

2. The prosecutor of the competent prosecutor's office, by an official act, accompanies and communicates the court decision to the electronic interception structure at the General Prosecution Office or Special Prosecution Office according to their competences.

3. The technical process of the listening and transcription may be conducted as well at the prosecution offices of the general jurisdiction and at the Special Prosecution Office according to their competences.

Article 24
Issuance of sub-legal acts
(Amended by law no. 69/2017 article 22)

The General Prosecutor, the Chief of the Special Prosecution Office, the minister responsible for public order and safety, the Minister of Defense, the Minister of Justice, the Minister of Finance, the Director of the National Information Service, the Director of the National Bureau of Investigation within 3 months of the establishment of the Special Prosecution Office, shall issue a joint instruction for:

- a) the detailed manner of conducting the interception process, in accordance with the requirements of Articles 6, 10, 13, 14 and 15 of this Law;
- b) the rules for secrecy and the documentation deriving from the interception process, pursuant to Articles 16 and 20 of this Law;
- c) the manner of preservation and destruction of the interception material, according to Article 20 of this Law.

Article 25
Transitory provision
(Provided by law no. 69/2017, article 23)

1. Within six months from the establishment of the Special Prosecution Office, the equipment that enables the technical processes of interception under this law, shall be installed at the premises of this prosecution office according to this law.

2. The Chief of the Special Prosecutor Office shall notify the High Judicial Council, the High Prosecutorial Council, the General Prosecution Office, and all institutions that carry out the interception of electronic communications under this law, the date when the electronic core command will start its functioning.

3. Within 10 days from the start of operation of the electronic core command, any

authorized interception and that is ongoing at the General Prosecution Office for criminal offenses under the jurisdiction of the Special Prosecution Office, shall be transferred to this prosecution office. Any other interception material for the cases under the competence of the Special Prosecution Office shall be transferred upon request at this prosecution office, unless when the material is destroyed in accordance with the provisions of this law.

4. Until the commencement of the functioning of the electronic command core at the Special Prosecution Office, its competences for the preventive interception of electronic communications shall be exercised by the General Prosecutor's Office.

5. Until the commencement of the functioning of the Appeal Court against Corruption and Organized Crime, the approval or refusal of a request for interception of electronic communications shall continue to be carried out by the General Prosecutor or, in his absence, by a prosecutor authorised by him.

Article 26 Abrogation

Every provision that falls in contradiction with this law shall be abrogated.

Article 27 Entry in force

This law shall enter into force 15 days after its publication into the Official Gazette.