

Law No. 124 of 3 August 2007

**“Intelligence System for the Security of the Republic  
and new Provisions governing Secrecy”**

Published in *Official Journal* no. 187 of 13 August 2007

Text in force as amended by Decree Law no. 85 of 2008 (confirmed, with amendments, by Law no. 121 of 2008) and Decree Law no. 78 of 2008 (confirmed, with amendments, by Law no. 102 of 2009)

Chapter I

STRUCTURE OF THE INTELLIGENCE SYSTEM FOR THE SECURITY OF THE REPUBLIC

Section 1

*(Powers of the President of the Council of Ministers)*

1. The following powers shall be vested exclusively in the President of the Council of Ministers:
  - a) Oversight of and overall responsibility for security intelligence policy in the interests and defence of the Republic and its underlying democratic institutions as established by the Constitution;
  - b) application of State-secret status and the protection of State secrets;
  - c) confirmation of the invocation of State-secret status;
  - d) the appointment and dismissal of the Director General and one or more Deputy Directors General of the Security Intelligence Department;
  - e) the appointment and dismissal of the Directors and Deputy Directors of the Security Intelligence Services; and
  - f) determination of the annual amount of financial resources to be allocated to the Security Intelligence Services and the Security Intelligence Department, which amount he/she shall communicate to the Parliamentary Committee referred to under section 30.
2. For the purposes of exercising the powers referred to under subsections (1) *b*) and *c*) above, the President of the Council of Ministers shall establish the criteria governing the application and the invocation of State-secret status and shall issue the provisions necessary for the administrative protection of State secrets, as well as those relating to the issue and revocation of security clearance.
3. The President of the Council of Ministers shall coordinate security intelligence policies, issue directives and, after prior consultation with the Interministerial Committee for the Security of the Republic, issue every measure necessary for the organization and operation of the Intelligence system for the security of the Republic.

Section 2

*(The Intelligence System for the Security of the Republic)*

1. The Intelligence System for the Security of the Republic shall comprise the President of the Council of Ministers, the Interministerial Committee for the Security of the Republic

(CISR – *il Comitato interministeriale per la sicurezza della Repubblica*), the Delegated Authority referred to under section 3 (where appointed), the Security Intelligence Department (DIS – *il Dipartimento delle informazioni per la sicurezza*), the External Security and Intelligence Agency (AISE – *l’Agenzia informazioni e sicurezza esterna*) and the Internal Security and Intelligence Agency (AISI – *l’Agenzia informazioni e sicurezza interna*).

2. For the purposes of this Act, “security intelligence services” means the AISE and the AISI.

### Section 3

#### *(The Delegated Authority)*

1. The President of the Council of Ministers may, if he/she considers it appropriate, delegate those functions not exclusively vested in him/herself solely to a Minister without Portfolio or to an Under-secretary of State, hereinafter referred to as the “Delegated authority”.
2. [repealed].
3. The President of the Council of Ministers shall be kept constantly informed by the Delegated Authority as to how the delegated functions are performed and, without prejudice to his/her power to issue directives, may take over the conduct of all or some of them at any time.
4. In derogation from the provisions of section 9(1) of Law no. 400 of 23 August 1988 (as subsequently amended), the opinion of the Council of Ministers is not required for the conferral of the delegated functions under this section upon the Minister without portfolio.

### Section 4

#### *(The Security Intelligence Department)*

1. The Security Intelligence Department (DIS) is hereby established within the Presidency of the Council of Ministers. It shall carry out the tasks referred to under subsection 3 below.
2. The President of the Council of Ministers and the Delegated Authority (where appointed) shall exercise their powers through the DIS, for the purposes of ensuring a fully unified approach in the Security Intelligence System’s planning of intelligence collection as well as in the Security Intelligence Services’ analyses and operational activities.
3. The DIS shall carry out the following tasks:
  - a) it shall coordinate all security intelligence activities and review the results of the activities carried out by the AISE and the AISI, without prejudice to the said services’ competence in intelligence collection and collaboration with foreign countries’ security services;
  - b) it shall keep itself constantly informed about the operations falling within the security intelligence services’ competence and shall pass the reports and analyses produced by the Security Intelligence System on to the President of the Council of Ministers;
  - c) it shall gather the information, analyses and reports arriving from the security intelligence services, from the Armed Forces and the police forces, from the State’s administrative entities and from research organizations, including private ones; without prejudice to the exclusive competence of the AISE and the AISI to draw

- d) partly on the basis of the intelligence and reports referred to under letter (c) above, it shall draw up overall analyses for submission to the CISR, as well as intelligence-collection projects, about which the President of the Council of Ministers shall decide, after obtaining the CISR's opinion;
- e) it shall promote and ensure (including by way of periodic meetings) the exchange of information between the AISE, the AISI and the police forces; it shall communicate the information acquired through the aforementioned exchange and the results of the periodic meetings to the President of the Council of Ministers;
- f) upon the instruction of the President of the Council of Ministers (after prior consultation with the CISR), it shall pass on intelligence and analyses to all those public administrative entities or bodies (including self-regulatory ones) that have an interest in acquiring security intelligence;
- g) in agreement with the AISE and the AISI, it shall draw up a plan for the acquisition of human and material resources and every other kind of resource instrumental to the security intelligence services' activities, to be submitted for approval by the President of the Council of Ministers;
- h) having consulted the AISE and the AISI, it shall draw up the draft Regulation referred to under section 21(1) of this Act and submit it for approval by the President of the Council of Ministers;
- i) it shall oversee the AISE and the AISI, checking that security intelligence activities comply with Acts of Parliament and with government Regulations, as well as with the directives and Provisions issued by the President of the Council of Ministers. To such end, an inspectorate shall be established within the DIS, the organization and operation of which shall be defined by the Regulation referred to under subsection (7) below. Within the scope of its powers as defined by the said Regulation, the inspectorate shall have the power to hold internal inquiries (including at the request of the DIS's Director General, when authorized by the President of the Council of Ministers) into specific episodes and instances of conduct occurring within the security intelligence services;
- l)<sup>1</sup> it shall ensure the correct application of the Provisions issued by the President of the Council of Ministers governing the administrative protection of state secrets;
- m) it shall see to institutional communications and the promotion and dissemination of a security awareness; and
- n) it shall issue guidelines for the unified management of the staff referred to under section 21 of this Act, in accordance with the specifications laid down in the Regulation referred to under section 21(1).

4. Without prejudice to the provisions of Article 118-*bis* of the Code of Criminal Procedure (introduced by section 14 of this Act), should the information requested of the Police Forces (in accordance with letters (c) and (e) of subsection 3 above) relate to inquiries conducted by the judicial police, such information, if covered by the secrecy protection provided by Article 329 of the Code of Criminal Procedure, may only be obtained with the

---

<sup>1</sup> Translator's note: in order to aid cross-referencing with the original Italian text, this English translation has adopted the Italian alphabet and the Italian system of inserting additional clauses into sections and articles (see, for example, the reference to Article 118-*bis* of the Code of Criminal Procedure in section 4(4) below).

prior authorization of the judicial authority with competence. The judicial authority may also transmit the records and information of his/her own initiative.

5. The Director General of the DIS shall be a top-echelon official or equivalent and his/her appointment and dismissal shall lie exclusively with the President of the Council of Ministers, after prior consultation with the CISR. The office shall be for a maximum term of four years and may be renewed only once. For the purposes of this Act, the Director General of the DIS shall report directly to the President of the Council of Ministers and the Delegated Authority (where appointed), save as provided for by section 6(5) and section 7(5) below, and he/she shall be the hierarchical and functional Head of the Staff working at the DIS and the offices established therein.
6. The President of the Council of Ministers shall, after consulting the Director General of the DIS, appoint one or more Deputy Directors General; the Director General shall make the other appointments within the Department, with the exception of those appointments that are to be made by the President of the Council of Ministers.
7. The structure and organization of the DIS and of the offices established therein shall be governed by a specific Regulation.
8. The Regulation provided for under subsection 7 above shall define the organization and operation of the inspectorate referred to under subsection 3 (i) above in accordance with the following criteria:
  - a) the inspectors shall be guaranteed full autonomy and independence of judgement in the exercise of their inspective duties;
  - b) save with the specific authorization of the President of the Council of Ministers or of the Delegated Authority, where appointed, inspection must not interfere with ongoing operations;
  - c) inspectors are to undergo a special selection process and receive appropriate instruction;
  - d) staff may not pass from the inspectorate to the Security Intelligence Services; and
  - e) with the prior authorization of the President of the Council of Ministers (or of the Delegated Authority, where appointed) inspectors shall have access to all the records kept by the security intelligence services and the DIS; they shall also have the right to obtain other information from public and private bodies through the Director General of the DIS.

## Section 5

### *(The Interministerial Committee for the Security of the Republic)*

1. An Interministerial Committee for the Security of the Republic (CISR) is hereby established within the Presidency of the Council of Ministers to advise, make proposals and take decisions regarding the lines and general goals of security intelligence policy.
2. The Committee shall draw up the general guiding principles and basic objectives to be pursued within the security intelligence policy framework and shall take decisions regarding the division of financial resources between the DIS and the Security Intelligence Services as well as regarding their related budgets and final accounts.

3. The Committee shall be chaired by the President of the Council of Ministers and shall comprise the Delegated Authority (where appointed), the Minister of Foreign Affairs, the Minister of the Interior, the Minister of Defence, the Minister of Justice, the Minister of Economy and Finance and the Minister of Economic Development.
4. The Director General of the DIS shall act as the Committee's secretary.
5. The President of the Council of Ministers may (including at their own request) call other members of the Council of Ministers, the Directors of the AISE and the AISI, as well as other civilian or military authorities whose presence may be considered necessary from time to time in relation to the issues on the agenda, to take part (without the right to vote) in the Committee's sessions.

## Section 6

### *(The External Security and Intelligence Agency)*

1. The External Security and Intelligence Agency (AISE) is hereby established. Its functions shall be to gather and process all intelligence falling within its areas of competence that serves to defend the independence, integrity and security of the Republic (including in implementation of international agreements) against threats originating abroad.
2. The AISE shall also be responsible for counter-proliferation activities concerning strategic materials as well as the security intelligence activities that are performed outside the national territory in order to protect Italy's political, military, economic, scientific and industrial interests.
3. The AISE shall also be responsible for identifying and countering outside national territory those espionage activities that are directed against Italy and those activities that are aimed at damaging national interests.
4. The AISE may carry out operations within the national territory only in collaboration with the AISI, where such operations are closely linked to activities that the AISE itself carries out abroad. To such end, the Director General of the DIS shall make provision to ensure the necessary forms of coordination and informational linkage, partly so as to avoid functional and territorial overlapping.
5. The AISE shall be directly answerable to the President of the Council of Ministers.
6. The AISE shall keep the Minister of Defence, the Minister of Foreign Affairs and the Minister of the Interior promptly and constantly informed regarding the profiles of their respective competences.
7. The President of the Council of Ministers shall, by way of decree after prior consultation with the CISR, appoint and dismiss the Director of the AISE, who shall be a top-echelon official or equivalent. The office of Director of the AISE shall be for a maximum term of four years and may be renewed only once.
8. The Director of the AISE shall report constantly on his agency's activities to the President of the Council of Ministers (or to the Delegated Authority, where appointed) through the Director General of the DIS. He shall report directly to the President of the Council of Ministers in cases of urgency or when other particular circumstances so require, informing the Director General of the DIS of such fact without delay. He shall submit an annual report on the Agency's operation and organization to the CISR, through the Director General of the DIS.
9. The President of the Council of Ministers shall appoint and dismiss one or more Deputy Directors, after consulting the Director of the AISE. The Director of the AISE shall make the other appointments within the Agency.
10. The organization and operation of the AISE shall be governed by a specific Regulation.

## Section 7

### *(The Internal Security and Intelligence Agency)*

1. The Internal Security and Intelligence Agency (AISI) is hereby established. Its functions shall be to gather and process all information falling within the areas of its competence that serves to defend the internal security of the Republic and its underlying democratic institutions as established by the Constitution (including in implementation of international agreements) from every threat, subversive activity and form of criminal or terrorist attack.
2. The AISI shall be responsible for the security intelligence activities that are carried out within the national territory in order to protect Italy's political, military, economic, scientific and industrial interests.
3. The AISI shall also be responsible for identifying and countering within the national territory those espionage activities that are directed against Italy and those activities that are aimed at damaging national interests.
4. The AISI may carry out operations abroad only in collaboration with the AISE, where such operations are closely linked to activities that the AISI is itself conducting within the national territory. To such end, the Director General of the DIS shall make provision to ensure the necessary forms of coordination and informational linkage, including for the purposes of avoiding functional and territorial overlapping.
5. The AISI shall be directly answerable to the President of the Council of Ministers.
6. The AISI shall keep the Minister of Defence, the Minister of Foreign Affairs and the Minister of the Interior promptly and constantly informed regarding the profiles of their respective competence.
7. The President of the Council of Ministers shall, after prior consultation with the CISR and by way of decree, appoint and dismiss the Director of the AISI, who shall be a top-echelon official or equivalent. The office of Director of the AISI shall be for a maximum term of four years and may be renewed only once.
8. The Director of the AISI shall report constantly on his agency's activities to the President of the Council of Ministers (or to the Delegated Authority, where appointed) through the Director General of the DIS. He shall report directly to the President of the Council of Ministers in cases of urgency or when other particular circumstances so require, informing the Director General of the DIS of such fact without delay. He shall submit an annual report on the Agency's organization and operation to the CISR, through the Director General of DIS.
9. The President of the Council of Ministers shall appoint and dismiss one or more Deputy Directors, after consulting the Director of the AISI. The Director of the AISI shall make the other appointments within the Agency.
10. The organization and operation of the AISI shall be governed by a specific Regulation.

## Section 8

### *(Exclusive nature of the functions attributed to the DIS, the AISE and the AISI)*

1. The functions attributed under this Act to the DIS, the AISE and the AISI may not be carried out by any other agency, body or office.

2. The Intelligence and Security Department of the General Defence Staff (RIS – *Reparto informazioni e sicurezza dello Stato maggiore della difesa*) shall carry out exclusively technical military tasks and military police tasks and, in particular, every form of intelligence activity serving to protect the facilities and activities of the Armed Forces abroad. It shall not be a part of the Security Intelligence System. The RIS shall act in close association with the AISE pursuant to Regulations issued by decree of the President of the Council of Ministers within 180 days from the date this Act comes into force, after prior deliberation by the CISR.

## Chapter II

### ORGANIZATIONAL PROVISIONS

#### Section 9

##### *(Administrative Protection of State Secrets and Security Clearance)*

1. The Central Secrecy Office (UCSe – *Ufficio centrale per la segretezza*) is hereby established within the DIS, in accordance with section 4 (7) of this Act. Its functions shall be to direct, coordinate, advise on and monitor the application of the Acts, Regulations and every other form of provision governing the administrative protection of State secrets and the secrecy classifications referred to under Section 42 of this Act.
2. The UCSe shall be responsible for:
  - a) the activities preliminary to exercise by the President of the Council of Ministers of his/her functions as the National Security Authority in protection of State secrets;
  - b) studying and preparing explanatory provisions directed at guaranteeing the security of everything covered by the secrecy classifications referred to under section 42 of this Act, with reference both to records, documents and other material, as well as to industrial production;
  - c) issuing and revoking security clearance (NOS – *nulla osta di sicurezza*), after obtaining the opinion of the Directors of the Security Intelligence Services and, where necessary, of the Minister of Defence and the Minister of the Interior; and
  - d) keeping and updating a full list of all parties issued with a NOS.
3. A NOS shall be valid for five years in relation to a “top secret” classification and for ten years in relation to “secret” and “confidential” secrecy classifications set out under section 42 of this Act, save where provided otherwise in international treaties that Italy has ratified. Each of the three secrecy classification shall be matched by a corresponding, separate level of NOS.
4. The issue of a NOS shall be subject to a preventive vetting procedure directed at excluding from access to classified information, documents, records or things every person whose rigorous observance of State secrecy and scrupulous loyalty to the Republic’s institutions and to the Constitution and its values cannot be fully relied upon.

5. For the purposes of facilitating the vetting referred to under subsection 4 above, the Armed Forces, the Police Forces, public administrative entities and bodies providing public utilities shall aid the UCSe in obtaining the information required to issue the NOSs, in accordance with sections 12 and 13 of this Act.
6. The UCSe shall have the power to revoke a NOS before expiry of the term referred to under subsection 3 above if, on the basis of information received or further vetting, the person concerned is shown to be unreliable.
7. The Regulation referred to under Section 4 (7) shall govern the preventive vetting procedure geared to the issue of a NOS referred to under subsection 4 of this Section, as well as the possible additional vetting referred to under subsection 6 above, and shall do so in such a way as to safeguard the rights of the persons concerned.
8. The persons concerned must be informed of the need for their vetting and can refuse to undergo it, thereby renouncing the NOS and the performance of the functions for which it is required.
9. The provisions contained in Section 17 (3) of the Code on Public Procurement relating to Works, Services and Supplies (contained in Legislative Decree no. 163 of 12<sup>th</sup> April 2006) shall apply to the procurement of works, goods and services for which the protection of secrecy may be required by Acts or Regulations or deemed necessary on an *ad hoc* basis.
10. The party contracting the works or supplies referred to under subsection 9 above, shall, when it considers it necessary, ask the President of the Council of Ministers (through the UCSe) for authorization to classify the matter as secret and shall state the reasons. The UCSe shall send the contracting party the list of individual providers and undertakings issued with a NOS at the same time that it sends the authorization.
11. The official in charge of the UCSe shall be appointed and dismissed by the President of the Council of Ministers, upon the proposal of the Delegated Authority (where appointed) and after prior consultation with the Director General of the DIS. Every year, the said official shall present the Director General of the DIS with a report on the work carried out and the problems tackled, on how well the Office's organization and procedures have complied with the tasks assigned it and on the measures to be adopted in order to ensure proper and efficient conduct. The Director General of the DIS shall inform the President of the Council of Ministers of the report and it shall be brought to the CISR's knowledge.

## Section 10

### *(Central Archives Office)*

1. The Central Archives Office is hereby established within the DIS, in accordance with section 4(7) of this Act. The Office shall:
  - a) implement the provisions governing the operation of and access to the archives kept by the Security Intelligence Services and the DIS;
  - b) manage the DIS's central archives;
  - c) oversee the security, upkeep and management of the afore-mentioned archives; and
  - d) be solely responsible for keeping, in special historical archives, the documentation relating to the Security Intelligence Services' activities and accounts, as well as the documentation regarding the forms of conduct referred to under section 17 and the related authorization procedures.



2. The Regulation referred to under section 4(7) shall define the organization and operation of the Central Archives Office, what procedures shall be followed for the computerization of paper documents and archives, how they are to be stored and accessed and the criteria for sending documentation to the State Central Archives.

## Section 11

### *(Instruction and Training)*

1. The Instruction School is hereby established within the DIS, in accordance with section 4(7) of this Act. It shall have the task of providing training, basic and continuing instruction and refresher courses to staff working in the DIS and the security intelligence services.
2. The School's directors shall include representatives from the Ministries concerned as well as qualified experts from university centres of excellence in the sectors of interest.
3. The Director General of the DIS, the Directors of the security intelligence services and the Director of the School shall define the instruction programmes annually in relation to the operational requirements of the security intelligence services, the changing international scenario and the evolving international strategic framework.
4. The School's Regulations shall define the manner and period of attendance at the said School, paying regard to the assignments to be performed within the Intelligence system for the security of the Republic and previous work experience.

## Section 12

### *(Co-operation of the Armed Forces and Police Forces)*

1. The Armed Forces, the Police Forces and the officers and agents working in the Judicial Police and law enforcement shall, within their respective fields of competence, offer the staff working in the security intelligence services every possible form of co-operation (including technical and operational co-operation) in the performance of their duties.
2. Without prejudice to the provisions of Article 118-*bis* of the Code of Criminal Procedure (introduced by section 14 of this Act), should the information requested of the Police Forces (in accordance with letters (c) and (e) of section 4(3) above) relate to inquiries conducted by the judicial police, such information, if covered by the secrecy protection provided by Article 329 of the Code of Criminal Procedure, may only be obtained with the prior authorization of the judicial authority with competence. The judicial authority may also transmit the records and information of his/her own initiative.
3. The Committee for anti-terrorist strategic analysis established within the Ministry of the Interior shall provide every possible form of co-operation to the Intelligence System for the Security of the Republic in the performance of its duties under this Act.

## Section 13

### *(Co-operation requested of public administrative entities and public utility providers)*

1. The DIS, the AISE and the AISI shall have the power to interact with all public administrative entities and the public utilities operating under an authorization, concession or agreement and request their co-operation (including logistical co-operation) where required to fulfil their own institutional duties; to such end, they shall have the power to draw up agreements with the said parties, as well as with universities and research organizations.
2. The provisions required to guarantee the DIS, the AISE and the AISI access to the computer archives kept by public administrative entities and by public utilities operating under an authorization, concession or agreement shall be issued in the form of a specific Regulation, after prior consultation with the administrative entities and utilities concerned. Such provisions shall, in any case, lay down the technical procedures by which it can be established (including subsequently) whether personal data has been accessed.
3. Under section 4(1) of Decree Law no. 144 of 27 July 2005 (confirmed, with amendments, by Law no. 155 of 31 July 2005), the words “or of mafia-related organized crime” shall be inserted after the words “constitutional system”.
4. Section 4 of Decree Law no. 144 of 27 July 2005 (confirmed, with amendments, by Law no. 155 of 31 July 2005 and amended by subsection (3) of this section) shall apply to the communications data.

#### Section 14

##### *(Introduction of Article 118-bis into the Code of Criminal Procedure)*

1. The following wording shall be inserted after article 118 of the Code of Criminal Procedure:  
  
*«Article 118-bis. – (Request for copies of records and information made by the President of the Council of Ministers). – 1. The President of the Council of Ministers shall have the power (including in derogation from the prohibition established by article 329 and either directly or through the Director General of the Security Intelligence Department) to request of the judicial authority with competence such copies of records of criminal proceedings and written information as to their contents as he/she deems indispensable for the performance of activities connected with the requirements of the Intelligence System for the Security of the Republic.*
2. The provisions of article 118(2) and (3) shall apply.
3. The judicial authority may also transmit the copies and information referred to under subsection (1) above of his/her own initiative. To the same ends, the judicial authority may grant direct access to the Register of Criminal Offences to officials delegated by the Director General of the Security Intelligence Department, even if the Register is kept in an automated form».

#### Section 15

##### *(Introduction of Article 256-bis into the Code of Criminal Procedure)*

1. The following wording shall be inserted after article 256 of the Code of Criminal Procedure:

«Article 256-bis. – (*Acquisition of documents, records or other things by a judicial authority on the premises of the security intelligence services*). – 1. When a judicial authority has to order the acquisition of documents, records or other things on the premises of the security intelligence services, in the Security Intelligence Department's offices or in offices connected with the performance of intelligence functions for the security of the Republic, the aforesaid judicial authority shall indicate the documents, records or things constituting the object of the request as specifically as possible in the production order.

2. The judicial authority shall carry out an on-site examination of the documents, records or things and shall admit to the evidence those that are strictly indispensable to the investigation. The judicial authority may request the assistance of judicial police officers when carrying out such an activity.

3. When the judicial authority has reason to believe that the documents, records or things produced are not those requested or that they are incomplete, he/she shall inform the President of the Council of Ministers. The President of the Council of Ministers shall take steps to arrange for the delivery of additional documents, records or things or, should the circumstances so require, to confirm the inexistence of additional documents, records or things.

4. When a document, record or thing originating from a foreign intelligence organization and passed on under a non-disclosure obligation needs to be acquired either in the original or in the form of a copy, the examination and immediate delivery shall be suspended and the document, record or thing shall be transmitted immediately to the President of the Council of Ministers so that the necessary steps may be taken with the foreign authority for the purpose of deciding on the application of State-secret status.

5. In the situation envisaged in subsection 4 above, the President of the Council of Ministers shall authorize the acquisition of the document, record or thing or shall invoke or confirm State-secret status within sixty days of the transmission.

6. Where the President of the Council of Ministers does not state his/her position within the time limit referred to under subsection 5 above, the judicial authority shall acquire the document, record or thing».

## Section 16

### *(Introduction of section 256-ter into the Code of Criminal Procedure)*

1. The following wording shall be inserted after article 256-bis of the Code of Criminal Procedure (introduced by section 15 of this Act):

«Article 256 –ter. - (*Acquisition of records, documents or other things regarding which State-secret status is claimed*). – 1. When documents, records or other things need to be acquired either in the original or in the form of a copy and the person in charge of the office holding them claims they have State-secret status, their examination and delivery shall be suspended; the document, record or thing shall be sealed in special containers and transmitted without delay to the President of the Council of Ministers.

2. In the situation envisaged in subsection 1 above, the President of the Council of Ministers shall authorize the acquisition of the document, record or thing or shall confirm its State-secret status within thirty days of the transmission.

3. If the President of the Council of Ministers does not state his/her position within the time limit referred to under subsection 2 above, the judicial authority shall acquire the document, record or thing.»

### Chapter III

## FUNCTIONAL GUARANTEES, LEGAL STATUS OF STAFF AND ACCOUNTING RULES

### Section 17.

#### *(Scope of the application of functional guarantees)*

1. Without prejudice to the provisions of article 51 of the Criminal Code, security intelligence services staff who adopt forms of conduct deemed by the law to constitute a criminal offence but that have been legitimately authorized on an *ad hoc* basis as indispensable to the institutional purposes of those services shall not be liable to punishment, provided that the limits set out under subsections 2, 3, 4 and 5 of this section and the procedures established under section 18 are rigorously observed.
2. The special justification provided for under subsection 1 above shall not apply if the conduct deemed by the law to constitute a criminal offence takes the form of crimes endangering or injuring the life, physical integrity, personal dignity, personal freedom, moral freedom, health or safety of one or more persons.
3. The special justification shall likewise not apply in cases of the criminal offences referred to under articles 289 and 294 of the Criminal Code or of crimes against the administration of justice, save where the conduct constitutes aiding the evasion of detection or aiding the profiting by a crime that is indispensable to the institutional purposes of the security intelligence services and is realized whilst rigorously observing the procedures established under section 18 and provided that such instances of aiding do not involve making false declarations to a judicial authority or concealing evidence of a crime and that they are not directed at misleading investigations ordered by a judicial authority. The special justification shall likewise not apply to the forms of conduct deemed to constitute a criminal offence pursuant to article 255 of the Criminal Code and Law no. 75 of 20 February 1958, as subsequently amended.
4. The forms of conduct deemed by the law to constitute a criminal offence in relation to which State-secret status may not be invoked (pursuant to section 39(11) of this Act, with the exception of the cases referred to under articles 270-*bis*(2) and 416-*bis*(1) of the Criminal Code) cannot be authorized pursuant to section 18 of this Act.
5. The forms of conduct referred to under subsection 1 above may not be carried out on the premises of political parties represented in Parliament or in a regional assembly or council, on the premises of trades-union organizations or in relation to officially registered professional journalists.
6. The special justification shall apply when the forms of conduct:
  - a) occur in the performance or on account of the security intelligence services' institutional tasks, in implementation of an operation that has been authorized and documented pursuant to section 18 and is carried out in accordance with the Security Intelligence System's organizational rules;
  - b) are indispensable and proportionate to the achievement of otherwise unachievable objectives in an operation;

- c) are the result of a thorough and objective weighing of the public and private interests involved; and
  - d) are carried out in such a way as to cause the minimum damage possible to affected interests.
7. When, on account of particular concrete situations and as a matter of exceptional necessity, the activities referred to in the present section are carried out by persons not employed by the security intelligence services, working together with one or more of the security intelligence services' employees, and the security intelligence services' recourse to their work is shown to have been indispensable and had been authorized in accordance with the procedures established by section 18, such persons are to be treated as the security intelligence services' staff, for the purposes of the application of the special justification.

## Section 18

*(Procedures for the authorization of conduct deemed by the law to constitute a criminal offence)*

1. Where the conditions referred to under section 17 are satisfied and the limits established therein have been rigorously observed, the President of the Council of Ministers (or the Delegated Authority, where appointed) shall authorize the forms of conduct deemed by the law to constitute a criminal offence and the operations of which they form a part.
2. The President of the Council of Ministers (or the Delegated Authority, where appointed) shall issue a reasoned authorization on the basis of a detailed request made by the Director of the Security Intelligence Service concerned. The said Director shall communicate such request in good time and inform the DIS of it. The requests and authorizations must be made in writing, partly for the purposes of preserving them in the filing system referred to under subsection 7.
3. The President of the Council of Ministers (or the Delegated Authority, where appointed) shall have the power, in any event, to amend or revoke the measure adopted pursuant to subsection 1. He/she shall use the same procedure as provided for under subsection 2.
4. In cases of absolute urgency where it is not possible to obtain the authorization referred to under subsection 2 in good time and a Delegated Authority has not been appointed, the Director of the Security Intelligence Service shall authorize the forms of conduct requested and shall communicate such fact immediately (or within twenty-four hours, in any event) to the President of the Council of Ministers (whilst informing the DIS of such fact), setting out the circumstances and the reasons for the urgent intervention.
5. If the President of the Council of Ministers or the Delegated Authority (where appointed and if the authorization fell within his/her competence) finds that the conditions referred to under section 17 have been satisfied and that the time limit for communication referred to under subsection 4 above has been observed, he/she shall ratify the measure within ten days.
6. In the cases where the forms of conduct deemed by the law to constitute a criminal offence have been carried out without or outside the scope of the authorizations provided for under this section, the President of the Council of Ministers shall take the necessary action and inform the judicial authorities without delay.

7. The documentation relating to the authorization requests provided for under this section shall be preserved within the DIS in a special, secret filing system, together with the documentation regarding the related expenses, in accordance with the rules issued under the Regulation referred to under section 4(7). The accounting relating to such expenses shall be submitted to a specific review carried out by the inspectorate within the DIS referred to under section 4(3)(i).

## Section 19

### *(Invocation of the special justification before a judicial authority)*

1. When preliminary investigations have been commenced in relation to some instance of the conduct indicated in section 17 which has been authorized pursuant to section 18, the Director of the Security Intelligence Service concerned shall (through the DIS) claim the existence of the special justification before the judicial authority proceeding with the investigation.
2. In cases of the type indicated in subsection 1, the public prosecutor shall immediately address a request to the President of the Council of Ministers, seeking confirmation that the authorization referred to under section 18 has been granted. The records relating to the investigation into the facts and those relating to the special justification shall be separated and entered in a special, confidential register so that they may be kept in a manner that protects their secrecy.
3. When the existence of the special justification is claimed during the course of a preliminary hearing or trial, the presiding judge shall address the relevant request for confirmation to the President of the Council of Ministers.
4. If the authorization has been granted, the President of the Council of Ministers shall communicate such fact to the relevant judicial authority within ten days and shall indicate the reasons. The confirmation shall immediately be communicated to the parliamentary Committee referred to under section 30. The case shall be suspended until the President of the Council of Ministers states the position.
5. If confirmation is not given within the time limit indicated in subsection 4, it shall be deemed to have been withheld and the judicial authority shall proceed in accordance with the ordinary provisions.
6. If the President of the Council of Ministers confirms the existence of the authorization, the judge shall, at the request of the prosecution or of his/her own will, dismiss the case or make an acquittal order, according to the circumstances of the case. The case's documentation shall be transferred to the public prosecutor who shall guard it in archives in a manner he/she shall determine as appropriate for the purposes of protecting its secrecy.
7. Where a conflict of competence issue is raised, a similar procedure for custody of the documentation shall be followed until the conflict has been resolved.
8. If a conflict of competence issue is raised, the Constitutional Court shall have full access to the documentation of the case and to the President of the Council of Minister's authorization measure, secrecy being guaranteed in a manner that the Court itself shall establish.
9. When the existence of the special justification is claimed by a person belonging to the Security Intelligence Services or by one of the parties referred to under section 17(7) at the moment when

he/she is caught in the act or when a preventive interim Court order is being executed, the measure's execution shall be suspended and the person shall be accompanied by the judicial police to their offices. He/she shall be detained there for the time strictly necessary for the first investigations to be made and for no longer than twenty-four hours in any event, save in the case provided for under subsection 10.

10. The public prosecutor shall immediately be informed and shall proceed in accordance with articles 390 et seq. of the Code of Criminal Procedure. He/she shall order the necessary inquiries and shall ask for confirmation from the Director General of the DIS. The Director General of the DIS must respond within twenty-four hours of the request. The person shall be held at the offices of the judicial police until confirmation shall arrive from the Director General of the DIS and for no more than twenty-four hours after receipt of the request, in any event. Once the time limit has expired without the requested confirmation having arrived, the procedure laid down by the Code of Criminal Procedure shall be followed.

11. If necessary, the public prosecutor shall request confirmation of the President of the Council of Ministers, who shall confirm or deny the existence of the special justification within ten days of the request. If confirmation is not received within the time limit indicated, it shall be deemed to have been withheld and the judicial authority shall proceed in accordance with the ordinary provisions.

## Section 20

### *(Criminal sanctions)*

1. Members of the Security Intelligence Services and the persons referred to under section 17(7) who illegally prearrange the conditions for the issue of an authorization pursuant to section 18, shall be punished with imprisonment for a term of between three and ten years.

## Section 21

### *(DIS and Security Intelligence Services Staff)*

1. A specific personnel group, established within the Presidency of the Council of Ministers and employed by the DIS and by the Security Intelligence Services, shall be provided for by way of a specific Regulation. The Regulation shall likewise govern the personnel's organization and recruitment (guaranteeing its unified management), the related pay and pensions and conditions of disclosure. It may do so in derogation from the legal provisions in force but shall observe the criteria established by this Act.

2. In particular, the Regulation shall provide for:

- a) the creation of a uniform category of personnel working in the Security Intelligence Services and the DIS: within such category administrative, operational and technical functions shall be distinguished;
- b) the definition of appropriate competitive examination and selection processes for personnel recruitment that are also open to citizens not employed within the public administration;

- c) the time limits for fixed-term employment (in observance of the laws in force) for those persons who, in accordance with letter *e*) below, are not employed through the competitive examination system;
- d) the identification of a quota of personnel called to directly assist the Director General of the DIS and the Directors of the Security Intelligence Services, whose tenure within the respective structures shall be tied to the tenure in office of the said directors;
- e) the prohibition against employing personnel directly, save in duly documented cases of particular, high-level specialization for activities that are strictly necessary to the operational effectiveness of the DIS and the Security Intelligence Services;
- f) the grounds for incompatibility, linked to the existence of kinship ties within three degrees or of relationship by marriage within two degrees or of cohabitation or of a proven shared economic interest with employees of the Security Intelligence Services or the DIS, save where the recruitment occurs by way of competitive examination system; should the kinship or in-law ties or cohabitation or shared economic interest concern the Director General of the DIS or the Directors of the Security Intelligence Services, the incompatibility shall be absolute;
- g) the prohibition against appointing to permanent posts any person who has, for any reason, terminated an employment relationship with the DIS or the Security Intelligence Services;
- h) the criteria for career advancement;
- i) the determination of the minimum percentage of employees on the roster referred to under letter *a*) for the DIS and for each service;
- l) the exceptional cases where assignments may be given to external experts, within the limits of and in relation to their particular professional profiles, fields of competence or specializations;
- m) the criteria and methodology governing the legal status and pay of personnel returning to the administrative entity of their previous employment, for the purposes of recognizing the professional skills acquired and the career advancement achieved; and
- n) the criteria and methodology for transferring members of the personnel referred to under letter *a*) to another administrative entity.

3. The rules provided for under Law no. 68 of 12<sup>th</sup> March 1999 (as subsequently amended) and by section 16 of Law no. 56 of 28 February 1987 (as subsequently amended) shall not apply to the recruitment of personnel employed by the DIS or the Security Intelligence Services.

4. Employment of personnel in violation of the prohibitions established under this Act or under the Regulation shall be null and void, without prejudice to the personal, economic and disciplinary liability of the person who arranged for such employment.

5. The Regulation shall define the quotas, the conditions and the methodology for transferring personnel from the General Secretariat of the CESIS, the SISMI and the SISDE into the staff category referred to under subsection 2(*a*).

6. The Regulation shall define the all-inclusive remuneration for personnel employed by the DIS, the AISE and the AISI within the limitations of the financial resources provided for under the legislation in force and without prejudice to the provisions of section 29(6) of this Act. Such remuneration shall comprise basic salary, special supplementary allowance, family allowance and a functional allowance, to be attributed according to rank, qualification and profile held as well as to the functions performed.



7. Any form of additional pay other than those provided for by the Regulation is forbidden. Should a member of the personnel return to his/her administrative entity of origin or be transferred to another public administrative entity, the main and additional pay due during employment with the Security Intelligence Services shall not be maintained, without prejudice to such measures as may have been adopted pursuant to subsection 2(m).
8. The Regulation shall govern the cases where either permanent or temporary employment is terminated.
9. The Regulation shall establish the conditions of ineligibility precluding an employment relationship with the DIS or with the Security Intelligence Services. It shall base such ineligibility on certain personal conditions, posts held or activities performed, providing for specific disclosure duties and, where these are breached, the consequential sanctions.
10. Persons whose scrupulous loyalty to the Constitution cannot be fully relied upon on account of subversive behaviour or actions towards democratic institutions, cannot carry out any form of activity under the Security Intelligence System's employment.
11. In no case shall the DIS or the Security Intelligence Services have the power (even occasionally) to employ the following persons directly or recruit them in a freelance or consultancy capacity: members of the European Parliament, the national Parliament or government; regional, provincial or municipal councillors or members of their respective executives; employees working within constitutional bodies, members of the judiciary, religious ministers and employed or freelance journalists.
12. All staff who work for the DIS or the Security Intelligence Services in any capacity are bound to preserve the secrecy of everything that has come to their knowledge in the exercise of or on account of their duties, even after the termination of such activity.

## Section 22

### *(Applications to the Court)*

1. Applications made to the Administrative judge in relation to disputes regarding the employer/employee relationship shall be governed by the provisions contained in section 23-bis of Law no. 1034 of 6 December 1971.

## Section 23

### *(Exclusion of the Status of Officer or Agent working in the Judicial Police or in Law Enforcement)*

1. The personnel referred to under section 21 shall not have the status of a Judicial Police officer or agent nor, save as provided for under subsection 2, that of a public security officer or agent. Those persons with such status in their administrative entity of origin shall have it suspended during the period of their employment within the specific group referred to under section 21.
2. The President of the Council of Ministers may attribute the status of public security officer or agent (with preventive policing duties) to some of the persons belonging to the specific group

referred to under section 21, in relation to the performance of activities that are strictly necessary for a specific operation of the Security Intelligence Services or directed at protecting personnel and structures of the DIS or the Security Intelligence Services. Such attribution shall be made upon the proposal of the Director General of the DIS and shall be for no longer than one year.

3. The attribution of such status may be renewed.
4. The attribution of such status shall be communicated to the Ministry of the Interior.
5. In urgent cases, the proposal of the Director General of the DIS may be made orally and followed by a written communication within twenty-four hours.
6. In derogation from the ordinary provisions, the personnel referred to under section 21 have the duty to report facts constituting a criminal offence to their respective directors. The said directors shall inform the President of the Council of Ministers (or the Delegated Authority, where appointed) without delay.
7. The Directors of the Security Intelligence Services and the Director General of the DIS have the duty to supply the competent organs of the judicial police with the information and evidence relating to those facts capable of constituting a criminal offence that have come to their knowledge within the structures for which they are respectively responsible.
8. With the authorization of the President of the Council of Ministers, performance of the duty referred to under subsection 7 may be delayed when such a delay is strictly necessary for the pursuit of the Security Intelligence System's institutional goals.

## Section 24

### *(Cover Identity)*

1. Upon the proposals of the Directors of the AISE and the AISI and after prior communication to the President of the Council of Ministers (or the Delegated Authority, where appointed), the Director General of the DIS may authorize members of the Security Intelligence Services to use identity documents containing personal details other than their true ones. The temporary use of cover documents and certificates may be ordered or authorized following the same procedure.
2. The documents indicated under subsection 1 shall not certify the status of agent or officer working in the Judicial Police force or in public security.
3. The methods for issuing and keeping the documents and certificates referred to under subsection 1, as well as the period of their validity, shall be defined by way of a specific Regulation. The DIS shall keep a confidential register attesting to the periods of validity and the procedures followed for issuing the documents and certificates referred to under subsection 1. At the end of an operation, the document or certificate shall be kept in a special archive set up within the DIS.

## Section 25

### *(Simulated Activities)*

1. Upon the proposals of the Directors of the AISE and the AISI and after prior communication to the President of the Council of Ministers (or the Delegated Authority, where appointed), the Director General of the DIS may authorize the exercise of simulated economic activities, either in the form of individual enterprises or in the form of companies of any kind.
2. The budget outturn for the activities referred to under subsection 1 shall be attached to the budget outturn for the secret Security Intelligence Services funds.
3. The manner in which the activities referred to under subsection 1 are to be carried out shall be established by a specific Regulation.

## Section 26

### *(Treatment of personal data)*

1. The gathering and treatment of data or information shall be directed solely at pursuing the Security Intelligence System's institutional goals.
2. The DIS, through the inspectorate referred to under section 4(3)(i), and the Directors of the Security Intelligence System shall ensure that the provisions of subsection 1 are observed.
3. Any member of the personnel employed by the Security Intelligence System who sets up or uses information files in any way that violates the provisions under subsection 1 shall be punished with imprisonment for a term of between three and ten years, if such action does not, of itself, constitute a more serious criminal offence.
4. The DIS, the AISE and the AISI shall not have the power to set up archives other than those whose existence has, in accordance with section 33(6), been officially communicated to the Parliamentary Committee referred to under section 30.

## Section 27

### *(Protection of Staff during Legal Proceedings)*

1. When, during the course of legal proceedings, statements have to be taken from a member of the Security Intelligence Services or the DIS, the judicial authority conducting the proceedings shall take every possible step to protect the person who has to be examined.
2. In particular, during the course of criminal proceedings, the judicial authority shall order the remote participation of the person referred to under subsection 1, whilst observing the provisions of section 146-*bis* of the transitional Rules implementing and coordinating the Code of Criminal Procedure contained in Legislative Decree no. 271 of 28 July 1989, insofar as they are compatible. The remote participation shall be ordered on condition that the appropriate technical instruments for permitting an audiovisual link are available and that the presence of the person is not necessary.
3. Article 128 of the Code of Civil Procedure and articles 472 and 473 of the Code of Criminal Procedure shall apply in any case, where the relevant conditions exist.

4. During the course of investigations, the public prosecutor shall nevertheless adopt the appropriate precautionary measures to protect the person who has to be examined or who has to participate in inquiry proceedings.

5. In particular, the public prosecutor shall always see that the secrecy of proceedings involving the participation of members of the Security Intelligence Services or DIS shall be preserved until the preliminary investigations have been closed, unless the preservation of secrecy totally obstructs the conduct of the investigations or there exists another significant reason for making the proceedings public. Such provision shall be made by way of an order briefly stating reasons and may derogate from the provisions of article 329(3) of the Code of Criminal Procedure.

6. During the course of the investigations, the public prosecutor shall likewise provide for the custody of the records referred to under this section in a manner appropriate to protecting their secrecy.

## Section 28

### *(Introduction of Article 270-bis into the Code of Criminal Procedure)*

1. The following wording shall be inserted after article 270 of the Code of Criminal Procedure:

«Article 270-bis. - *(Service communications by members of the Security Intelligence Department or the Security Intelligence Services)*. - 1. When a judicial authority has, by interception, obtained service communications made by members of the Security Intelligence Department or the Security Intelligence Services, he/she shall order that the documents, media and records concerning such communications are immediately to be classified as a secret and guarded in a protected place.

2. Once interception has been concluded, the judicial authority shall send the President of the Council of Ministers a copy of the documentation containing the information he/she intends to use at trial and shall ascertain whether any of the information has State-secret status.

3. Before the President of the Council of Ministers replies, the information sent to him/her may only be used if there is a danger of tampering with evidence or of flight or when intervention is necessary to prevent or interrupt the commission of a crime punishable with imprisonment for a maximum term of not less than four years, without prejudice to the law governing the special justification envisaged for the activities of the Security Intelligence Services' personnel.

4. If the President of the Council of Ministers does not invoke State-secret status within sixty days of being notified of the request, the judicial authority shall acquire the information and provide for the case to continue.

5. Invocation of State-secret status shall bar the judicial authority from using the information having State-secret status.

6. It shall, in any case, remain open to the judicial authority to proceed on the basis of elements existing separately and independently of the information having State-secret status.

7. Where a conflict of competence issue is raised against the President of the Council of Ministers, should the conflict result in a finding that no State secret exists, the President of the Council of Ministers shall not have the power to invoke State-secret status again in relation to the same matter. Should the conflict result in a finding that a State secret does exist the judicial authority shall have no power either to acquire or to use (whether directly or indirectly) records or documents in relation to which State-secret status has been invoked.

8. In no circumstances may State-secret status be invoked against the Constitutional Court. The Court shall adopt the necessary measures to ensure the secrecy of its proceedings.»

## Section 29.

### *(Accounting Rules and Financial Provisions)*

1. A specific basic allocation for the Security Intelligence System's expenses shall be established within the estimate for the Ministry of Economy and Finance.

2. At the beginning of the fiscal year, after prior deliberation by the CISR following consultation with the persons in charge of the DIS, the AISE and the AISI, the President of the Council of Ministers shall apportion the allocated funds referred to under subsection 1 between the said bodies. He shall likewise determine the amounts to be allocated to the ordinary funds and to the secret ones. Such apportionment and any variations during the course of the year to be adopted under the same procedure shall be communicated to the Parliamentary Committee referred to under section 30.

3. The Regulation governing the DIS and the Security Intelligence Services' accounting shall be adopted after prior consultation with the President of the Court of Auditors. It may derogate from the general State accounting rules but shall observe both the basic principles those rules establish and the following provisions:

- a) there shall be one budget, in which the funds for the confidential expenses shall be indicated as a separate item, and one set of final accounts for the ordinary expenses for the DIS, the AISE and the AISI and they shall be prepared upon the proposals of the persons in charge of the said structures, each person in relation to the area of his/her respective competence;
- b) the President of the Council of Ministers shall adopt the budget and the final accounts referred to under (a) by way of decree, after prior deliberation by the CISR;
- c) the final accounts (together with the annual report of the internal auditing body) shall be sent to a branch office of the Court of Auditors operating within the DIS, so that their legality and regularity may be checked. Such branch office shall be organized pursuant to Section 98 of Royal Decree no. 1214 of 12 July 1934 (including in derogation from the provisions referred to under section 10(10) of Law no. 117 of 13 April 1988). Said branch office shall be responsible for the activities preliminary to the legality audit of records pursuant to section 3(2) of Law no. 20 of 14 January 1994;
- d) the records of the ordinary expenses' administration shall be subject to a preliminary audit by a branch office operating within the DIS and reporting to the Budget and Accounting Office at the Presidency of the Council of Ministers;
- e) the persons working in the branch offices of the Court of Auditors and the Budget and Accounting Office at the Presidency of the Council of Ministers referred to under letters (c) and (d) shall be individually appointed by the President of the Court of Auditors and the

President of the Council of Ministers, respectively, and shall be bound to observe State secrecy;

- f) the records of the confidential expenses' administration shall be approved solely by the persons in charge of the DIS and the Security Intelligence Services. Such persons shall present a specific quarterly report and an annual final report to the President of the Council of Ministers; and
- g) the final accounts for the financial administration of the ordinary expenses shall be transmitted, together with the Court of Auditors' report, to the Parliamentary Committee referred to under section 30. The said Committee shall also be presented with a report on the essential individual posts of the financial administration of the confidential expenses, to be included in the half-yearly report referred to under section 33 (1) of this Act. The documentation relating to the confidential expenses shall not indicate names and shall be kept in the historical archives referred to under section 10(1)(d) of this Act.

4. The procedures for drawing up procurement contracts for works, goods and services in compliance with the provisions of section 17 of the Code on Public Contracts relating to Works, Services and Supplies, contained in Legislative Decree no. 163 of 12<sup>th</sup> April 2006, as amended by subsection 5 of this section, shall be defined by way of a specific Regulation. The works, supplies and services that, on account of their nature or value, may be carried out on a time and material basis or by way of private negotiation shall also be identified.

5. Article 17(8) of the Code contained in Legislative Decree no. 163 of 12<sup>th</sup> April 2006 is hereby repealed.

6. Implementation of this Act must not generate new or increased burdens on public finance.

## Chapter IV

### PARLIAMENTARY OVERSIGHT

#### Section 30

##### *(Parliamentary Committee for the Security of the Republic)*

1. A Parliamentary Committee for the Security of the Republic is hereby established. It shall be composed of five Deputies and five Senators who are to be appointed by the Presidents of the two Houses of Parliament within twenty days of the opening of every Parliament. The said Committee's composition shall reflect the number of members in the parliamentary groups, whilst ensuring the equal representation of both the majority and the opposition groups and taking the specific nature of the Committee's tasks into account.

2. The Committee shall constantly and systematically verify that the Security Intelligence System's activities are carried out in observance both of the Constitution and of the law and in the defence and exclusive interests of the Republic and its institutions.

3. The Committee's Bureau shall comprise a Chairperson, a Deputy-Chairperson and a Secretary who shall be elected by the Committee members by way of a secret ballot. The Chairperson shall

be elected from amongst the members belonging to the opposition groups and he/she must be elected by an absolute majority.

4. If no candidate achieves such a majority, a second ballot shall then be held between the two candidates who received the greatest number of votes.

5. In cases where candidates receive an equal number of votes, the candidate who is senior in age shall be declared elected or shall go forward to the second ballot.

6. As regards the election of the Deputy-Chairperson and the Secretary, respectively, every member shall write a single name on his/her ballot paper. The persons who receive the greatest number of votes shall be elected. In cases where candidates receive an equal number of votes, the procedure established under subsection 5 shall be followed.

### Section 31

#### *(Oversight Functions of the Parliamentary Committee for the Security of the Republic)*

1. In performance of its functions, the Parliamentary Committee for the Security of the Republic shall periodically hear the President of the Council of Ministers (and the Delegated Authority, where appointed), the Ministers forming the CISR, the Director General of the DIS and the Directors of the AISE and the AISI.

2. The Committee shall likewise have the right, in exceptional cases, to provide by way of a reasoned decision for the hearing of persons employed by the Security Intelligence System. The decision shall be communicated to the President of the Council of Ministers who may, under his/her own responsibility, oppose the holding of the hearing, stating the reasons therefor.

3. The Committee shall likewise have the power to hear any other person (not belonging to the Security Intelligence System) who is able to provide information or assessments deemed useful to the exercise of Parliamentary oversight.

4. All persons heard shall report the information in their possession regarding matters of interest to the Committee both truthfully and fully.

5. The Committee shall have the power (including in derogation from the prohibition under article 329 of the Code of Criminal Procedure) to obtain copies of records or documents relating to proceedings or inquiries being conducted by a judicial authority or some other investigative body, as well as copies of records or documents relating to parliamentary investigations or inquiries. The judicial authority may also transmit copies of records or documents of his/her own initiative.

6. The judicial authority shall promptly provide for transmission of the documentation requested pursuant to subsection 5, unless he/she gives notice, by way of an order stating reasons of a preliminary evidentiary nature, of the need to delay such transmission. When the reasons for the postponement no longer exist, the judicial authority shall transmit everything requested without delay. Orders shall be effective for six months and may be renewed but shall become ineffective once the preliminary inquiries have been closed.

7. The Committee shall have the power to obtain information of interest to it from members of the Security Intelligence System and from public administrative bodies and offices, as well as copies of records and documents kept, produced or, in any event, acquired by them.

8. Should the communication of a piece of information or the transmission of a copy of a document risk prejudicing the security of the Republic, relations with foreign States, the conduct of ongoing operations or the safety of sources, external staffers or members of the Security Intelligence Services, the recipient of the request shall invoke the need to maintain confidentiality before the Committee.
9. Where the Committee considers it appropriate to insist on its request, such request shall be submitted to the President of the Council of Ministers for his/her assessment. The President of the Council of Ministers shall decide within thirty days whether the need invoked actually exists. In no circumstances can confidentiality be invoked or confirmed in relation to facts for which State Secret status may not be invoked. In no circumstances can State-secret status or the need for confidentiality referred to under subsection 8 be invoked before the Committee when, by unanimous vote, it has called for investigations as to whether the behaviour of the Security Intelligence Services' members corresponds to the institutional duties established by this Act.
10. Should the Committee consider the President of the Council of Ministers' decision to be unfounded or should it fail to receive any communication within the prescribed timeframe, it shall report on the matter to both of the Houses for their assessment of the situation.
11. Without prejudice to the provisions of subsection 5, neither civil service secrecy nor banking or professional secrecy can be invoked before the Committee, save in the case of the confidentiality duty owed by defence counsel to his/her client within the scope of his/her brief in legal proceedings.
12. When requested information, records or documents have been made subject to a functional secrecy restriction by the Parliamentary Committees of Inquiry with competence, such secrecy restriction cannot be invoked before the Committee.
13. The Committee shall have the power to audit directly the expenses documentation for completed operations. To such end, it shall access the DIS's central archives referred to under section 10 (1)(b).
14. The Committee shall have the power to access and carry out on-the-spot checks in the offices falling within the Security Intelligence System's competence. It shall communicate such actions to the President of the Council of Ministers in advance.
15. In the circumstances envisaged under subsection 14, the President of the Council of Ministers shall have the power to postpone access should there exist the risk of interference with continuing operations.

## Section 32

### *(Consultative Functions of the Parliamentary Committee for the Security of the Republic)*

1. The Parliamentary Committee for the Security of the Republic shall give its opinion of the draft Regulations provided for by this Act, as well as of every other draft Decree or draft Regulation concerning the organization and status of the specific personnel group referred to under section 21.



2. The President of the Council of Ministers shall give the Chairperson of the Parliamentary Committee for the Security of the Republic advance notice of the appointments of the Director General and Deputy Directors General of the DIS and of the Directors and Deputy Directors of the Security Intelligence Services.
3. The opinions referred to under subsection 1 shall be mandatory but not binding.
4. The Committee shall give the opinions referred to under subsection 1 within one month of receiving the draft Decree or draft Regulation; such timeframe may be extended only once by not more than fifteen days.

### Section 33

#### *(Duties to Communicate to the Parliamentary Committee for the Security of the Republic)*

1. Every six months, the President of the Council of Ministers shall send a report on the Security Intelligence Services' activities to the Parliamentary Committee for the Security of the Republic. The report shall contain an analysis of the situation and of the dangers threatening security.
2. The DIS shall send to the Committee all the Regulations and Directives issued by the President of the Council of Ministers regarding the subject-matters falling within the Committee's competence, as well as the Decrees and Regulations concerning the organization and status of the specific personnel group referred to under section 21.
3. The Minister of the Interior, the Defence Minister and the Minister of Foreign Affairs shall send the Committee the Regulations that they issue in relation to the Security Intelligence System's activities.
4. The President of the Council of Ministers shall inform the Committee about those operations conducted by the Security Intelligence Services in which forms of conduct have been adopted that are deemed by the law to constitute a criminal offence but have been authorized pursuant to section 18 of this Act and section 4 of Decree Law no. 144 of 27 July 2005 (confirmed, with amendments, by Law no. 155 of 31 July 2005). The information shall be sent to the Committee within thirty days of the date that the operations are concluded.
5. The President of the Council of Ministers shall promptly communicate to the Committee all the inquiries made pursuant to article 270-bis of the Code of Criminal Procedure (introduced by section 28 of this Act) and the resulting determinations adopted.
6. The President of the Council of Ministers shall promptly communicate to the Committee the establishment of the archives for the DIS and the Security Intelligence Services.
7. In his report on each half-year, the President of the Council of Ministers shall provide information to the Committee on the DIS's and the Security Intelligence Services' financial administration for the same half-yearly period.
8. The information referred to under subsection 7 shall summarize, under aggregated headings covering homogeneous categories of expenditure, the forecasts recorded in the budget for the DIS, the AISE and the AISI and the relative actual expenditure.

9. In his half-yearly report, the President of the Council of Ministers shall inform the Committee of the criteria governing the acquisition of the personal data collected by the Security Intelligence Services in pursuit of their goals.

10. Every year, the President of the Council of Ministers shall present his report on the first six months of the year in progress by 30 September of that year. Every year, the President of the Council of Ministers shall present his report on the second six months of the year by 31 March of the following year.

11. In his second half-yearly report, the President of the Council of Ministers shall send the Committee information on essential aspects of the activities carried out during the preceding year pursuant to section 24(1).

12. The half-yearly report shall also provide information on the number of staff and the recruitment of personnel during the half-year period of reference, as well as on the cases of direct appointments, indicating the criteria and the selection procedure adopted.

#### Section 34

##### *(Ascertainment of Unlawful or Irregular Conduct)*

1. Should the Parliamentary Committee for the Security of the Republic, in the exercise of its duties, discover forms of conduct that have violated the rules governing security intelligence activities, it shall inform the President of the Council of Ministers and report the matter to the Presidents of the Houses of Parliament.

#### Section 35

##### *(Reports submitted by the Parliamentary Committee for the Security of the Republic)*

1. The Parliamentary Committee for the Security of the Republic shall present Parliament with an annual report which shall give an account of its activities and formulate proposals or observations regarding issues within its competence.

2. The Parliamentary Committee for the Security of the Republic shall also have the power to send Parliament urgent information or reports during the year.

#### Section 36

##### *(Duty to preserve secrecy)*

1. The members of the Parliamentary Committee for the Security of the Republic, the civil servants and personnel of any grade or rank whatsoever who are attached to the said Committee and all persons who assist the Committee or who, by virtue of their office or duties, come to know about the Committee's activities shall be bound to preserve the secrecy of the information acquired, even after their task has ended.

2. Breach of the secrecy duty referred to under subsection 1 shall be punished in accordance with the provisions of article 326 of the Criminal Code, save where such fact constitutes a more serious criminal offence. If the breach is committed by a Member of Parliament, the penalty shall be increased by between one third and one half.
3. Save where such fact constitutes a more serious criminal offence, the penalties provided for under article 326 of the Criminal Code shall also apply to whoever discloses, either wholly or in part, records or documents whose disclosure has not been authorized.
4. The Chairperson of the Committee shall report breaches of the secrecy duty referred to under subsection 1 to the judicial authorities, including at the request of one of his/her committee members.
5. Without prejudice to the provisions of subsection 4, should it be clearly shown that the breach is attributable to one of the Committee's members, the Chairperson of the Committee shall inform the Presidents of both Houses.
6. After receiving the information referred to under subsection 5, the President of the House to which the Member of Parliament concerned belongs shall appoint a Commission of Inquiry. Such Commission of Inquiry shall be composed of parliamentarians from the majority and the opposition groups in equal numbers.
7. The Commission of Inquiry referred to under subsection 6 shall proceed in accordance with the Procedural Rules for the House to which the Member of Parliament concerned belongs. It shall report its conclusions to the President of the House. Should the Commission consider that the Member of Parliament concerned has breached the secrecy duty, the President of the House to which the said member belongs shall proceed to replace him/her in his/her capacity as a member of the Committee, observing the criteria established under section 30(1) and after prior communication of such substitution to the President of the other House of Parliament.

## Section 37

### *(Internal Organization)*

1. The activities and operation of the Parliamentary Committee for the Security of the Republic shall be governed by internal Rules of Procedure, approved by an absolute majority of the said Committee's members. Every member shall have the power to propose amendments to the said procedural Rules.
2. The Committee's sittings and all its records shall be secret, save where the Committee itself decides otherwise.
3. The records and documents obtained by the Committee shall be subject to the regime established by the authority that created them.
4. In order to perform its functions, the Committee shall make use of personnel, premises and operational tools provided by the Presidents of the Houses, in agreement between themselves. The archives and all the records of the Parliamentary Committee referred to under s. 11 of Law 801 of 24 October 1977 shall be transferred to the Parliamentary Committee for the Security of the Republic.

5. The Committee's operational expenses shall be determined in a manner that reflects the new duties assigned it and shall be borne by the Senate of the Republic's internal budget as to one half and by the Chamber of Deputies' internal budget as to the other half. The Committee may have recourse to those forms of external support or assistance it considers necessary, after prior communication to the Presidents of the Houses of Parliament and within the limits of the financial resources allocated. The Committee may not, in any way, have recourse to the assistance of members or ex-members of the Security Intelligence System or of persons who are assisting or have assisted Foreign States' Intelligence bodies.

### Section 38

*(Report to Parliament)*

1. By the end of February each year, the Government shall send Parliament a written report on its security intelligence policy and results achieved for the previous year.

### Chapter V

#### PROVISIONS GOVERNING STATE SECRETS

### Section 39

*(State-Secret Status)*

1. The records, documents, information, activities and every other thing the disclosure of which may be used to damage the integrity of the Republic (including in relation to international agreements, the defence of its underlying institutions as established by the Constitution, the State's independence *vis à vis* other states and its relations with them, as well as its military preparation and defence), shall have State-secret status.

2. The information, documents, records, activities, things and places having State-secret status shall be made known solely to the persons and authorities called to carry out essential functions in their regard, to the extent and within the limits that are indispensable for performing their respective tasks and achieving respectively established goals. All records and documents concerning state secrets must be kept using appropriate devices for preventing their being tampered with, removed or destroyed.

3. The information, documents, records, activities, things or places the knowledge of which outside authorized environments and offices would seriously prejudice the objectives referred to in subsection 1 shall have State-secret status.

4. The restriction deriving from State-secret status shall be applied, upon the express provision of the President of the Council of Ministers, to the records, documents or things that are the object of it, even if they have been obtained abroad. Where possible, such restriction shall be recorded on the items subject to it.

5. In implementation of the rules established under this Act, the President of the Council of Ministers shall regulate the criteria for identifying the information, documents, records, activities, things and places to which State-secret status may apply. He shall do so by way of a Regulation.
6. Through the Regulation referred to under subsection 5, the President of the Council of Ministers shall identify the offices with competence to carry out those inspections on places having State-secret status that are usually carried out by the local health authorities and the national fire brigade.
7. After the expiry of fifteen years from the moment of application of State-secret status or, failing that, from an invocation of State-secret status that is confirmed in accordance with article 202 of the Code of Criminal Procedure (as substituted by section 40 of this Act), any person who has an interest may ask the President of the Council of Ministers to be allowed access to the information, documents, records, activities, things or places having State-secret status.
8. Within thirty days of the request, the President of the Council of Ministers shall allow the access or shall provide, by way of a measure stating reasons, to be sent without delay to the Parliamentary Committee for the Security of the Republic, for one or more extensions of the restriction. The overall duration of a State-secret status restriction shall not exceed thirty years.
9. Independently of the expiry of the time limits referred to under subsections 7 and 8, the President of the Council of Ministers shall provide for the restriction to be lifted when the requirements that determined the application no longer exist.
10. When, on the basis of international agreements, the existence of State-secret status also affects the interests of foreign States or international organizations, the measure providing for the restriction to be lifted shall be adopted after prior agreement with the competent foreign or international authorities, save where there exist exceptionally serious reasons to the contrary and subject to reciprocity.
11. In no circumstances shall information, documents or matters relating to acts of terrorism, acts subverting the constitutional order or acts constituting the criminal offences referred to under articles 285, 416-*bis*, 416-*ter* and 422 of the Criminal Code have State-secret status.

## Section 40

### *(Protection of State secrets)*

1. Article 202 of the Code of Criminal Procedure shall be substituted by the following:  
  
«Article 202. – *(State secrets)*. - 1. Public officials, civil servants and public service providers shall have the duty to refrain from giving evidence about facts having State-secret status.  
2. If a witness invokes State-secret status, the judicial authority shall suspend every initiative directed at acquiring the information having State-secret status and shall inform the President of the Council of Ministers for the purposes of receiving confirmation, where appropriate.  
3. Should State-secret status be confirmed and should knowledge of the matters having State-secret status be shown to be essential to the conclusion of the proceedings, the judicial authority shall state that he/she cannot proceed because of the existence of a State secret.  
4. If the President of the Council of Ministers fails to confirm State-secret status within thirty days of receiving notification of the request, the judicial authority shall acquire the information and provide for the proceedings to continue.

5. An invocation of State-secret status that is confirmed by the President of the Council of Ministers in a document stating reasons shall bar the judicial authority from acquiring and using the information having State-secret status even indirectly.

6. It shall, in any case, remain open to the judicial authority to proceed on the basis of elements existing separately and independently of the records, documents or matters having State-secret status.

7. Where a conflict of competence issue is raised against the President of the Council of Ministers, should the conflict result in a finding that no State secret exists, the President of the Council of Ministers shall not have the power to invoke State-secret status again in relation to the same matter. Should the conflict result in a finding that a State secret does exist, the judicial authority shall have no power either to acquire or to use (whether directly or indirectly) records or documents in relation to which State-secret status has been invoked.

8. In no circumstances may State-secret status be invoked against the Constitutional Court. The Court shall adopt the necessary measures to ensure the secrecy of its proceedings.»

2. The following wording shall be added to the end of the first sentence of article 204(1) of the Code of Criminal Procedure: «as well as the criminal offences provided for under articles 285, 416-*bis*, 416-*ter* and 422 of the Criminal Code».

3. The following paragraphs shall be inserted after the first paragraph of article 204 of the Code of Criminal Procedure:

*1-bis.* Acts, information or documents concerning forms of conduct that are adopted by members of the Security Intelligence Services in violation of the law governing the special justification provided for the activities of Security Intelligence Services personnel cannot have the State-secret status provided for by articles 201, 202 and 203. Those forms of conduct in relation to which the existence of the special justification is shown to be impossible (after following the specific, legally established procedure) shall be deemed violations of the abovementioned law.

*1-ter.* State-secret status cannot be invoked or confirmed solely in order to protect a secrecy classification or solely by virtue of the nature of the document, record or thing classified.

*1-quater.* In no circumstances may State-secret status be invoked against the Constitutional Court. The Court shall adopt the necessary measures to guarantee the secrecy of its proceedings.

*1-quinquies.* When the President of the Council of Ministers does not consider it appropriate to confirm State-secret status, he/she shall, in his/her capacity as National Security Authority, take steps to declassify the records, documents, things or places classified as secret before they are made available to the competent judicial authority».

4. The following amendments shall be made to section 66 of the transitional Rules implementing and coordinating the Code of Criminal Procedure contained in Legislative Decree no. 271 of 28 July 1989:

*a)* paragraph 2 shall be substituted by the following:

«2. When the communication provided for under article 204(2) of the Code arrives, if the President of the Council of Ministers considers that the conditions indicated in paragraphs 1, 1-*bis* and 1-*ter* of the same article do not exist (because the fact, information or document having State-secret status does not concern the criminal offence in relation to which proceedings have been instituted), he/she shall confirm State-secret status in a document stating reasons. Should he/she fail to do so within thirty days of the communication's notification, the judge may order seizure of the document or the examination of the party concerned.»;

*b)* Paragraph 3 is repealed.

5. The President of the Council of Ministers shall be bound both to communicate to the Parliamentary Committee referred to under section 30 of this Act every case where an invocation of State-secret status is confirmed, pursuant to article 202 of the Code of Criminal Procedure (as substituted by subsection 1 of the present section) or to article 66 (2) of the transitional Rules implementing and coordinating the Code of Criminal Procedure (contained in Legislative Decree no. 271 of 28 July 1989), and to give the essential reasons for such confirmation. If the Committee considers the invocation of State-secret status to be groundless, it shall report the matter to both Houses of Parliament for their assessment of the situation.

#### Section 41

##### *(Prohibition against relating facts having State-secret status)*

1. Public officials, public employees and public service providers are forbidden to relate facts having State-secret status. If State-secret status has been invoked at any stage of criminal proceedings then, without prejudice to the provisions contained in article 202 of the Code of Criminal Procedure (as substituted by section 40 of this Act), the judicial authority shall inform the President of the Council of Ministers (in his/her capacity as National Security Authority), so that the necessary decisions falling within his/her competence may be taken.
2. If the judicial authority considers that knowledge of the matters having State-secret status is essential for the conclusion of the proceedings, he/she shall suspend every initiative directed at acquiring the information having State-secret status and ask the President of the Council of Ministers to confirm the existence of State-secret status.
3. Should State-secret status be confirmed and should knowledge of the matters having State-secret status be shown to be essential for the conclusion of the proceedings, the judge shall state that he/she cannot proceed on account of the existence of a State secret.
4. If the President of the Council of Ministers fails to confirm State-secret status within thirty days of receiving notification of the request, the judicial authority shall acquire the information and make provision for the proceedings to continue.
5. An invocation of State-secret status that is confirmed by the President of the Council of Ministers in a document stating reasons shall bar the judicial authority from acquiring or using the information having State-secret status even indirectly.
6. It shall, in any case, remain open to the judicial authority to proceed on the basis of elements existing separately and independently of the records, documents or matters having State-secret status.
7. Where a conflict of competence issue is raised against the President of the Council of Ministers, should the conflict result in a finding that no State secret exists, the President of the Council of Ministers shall not have the power to invoke State-secret status again in relation to the same material. Should the conflict result in a finding that a State secret does exist, the judicial authority shall have no power either to acquire or to use (whether directly or indirectly) records or documents in relation to which State-secret status has been invoked.
8. In no circumstances may State-secret status be invoked against the Constitutional Court. The Court shall adopt the necessary measures to guarantee the secrecy of its proceedings.

9. The President of the Council of Ministers shall be bound both to communicate to the Parliamentary Committee referred to under section 30 every case where an invocation of State-secret status is confirmed pursuant to this section, and to give the essential reasons for such confirmation. If the Parliamentary Committee considers the invocation of State-secret status to be groundless, it shall report the matter to both Houses of Parliament for their assessment of the situation.

## Section 42

### *(Secrecy classifications)*

1. Secrecy classifications shall be attributed for the purposes of limiting the knowledge of information, documents, records, activities or things solely to those persons who need to have access to them by virtue of their personal institutional functions.

1-bis. For the purposes of handling information classified as “top secret”, “secret” and “confidential”, possession of NOS shall be also required

2. The secrecy classification shall be applied (and may be upgraded) by the authority who creates the document or record or first acquires the information, is responsible for the thing or acquires documents, records, information or things from abroad.

3. The attributable classifications shall be: “top secret”, “secret”, “confidential” and “restricted”. The classifications shall be attributed according to the criteria ordinarily followed in international relations.

4. The person who applies the secrecy classification shall identify the parts within every record or document that must be classified and shall specifically establish the level of classification corresponding to each separate part.

5. A secrecy classification shall automatically be downgraded to a lower classification level upon the expiry of five years from the date of its original application. Once a further five-year period has expired, all classification restrictions shall be lifted.

6. Automatic declassification shall not apply when, by way of a measure stating reasons, the restriction’s duration is extended by the person who effected the original classification or, in cases of extension beyond a term of fifteen years, by the President of the Council of Ministers.

7. The President of the Council of Ministers shall verify that the rules governing secrecy classifications are observed. The scope of the individual levels of secrecy, the persons who shall be granted the power to classify and the offices that, within the public administration, are linked to the performance of intelligence functions for the security of the Republic shall be determined by a specific Regulation, as shall the criteria for identifying the subject matters to be classified and the manner of accessing them in military places or those defined as of interest for the security of the Republic.

8. Should a judicial authority order the production of classified documents in relation to which State-secret status is not invoked, the documents shall be delivered to the judicial authority requesting them. The said judicial authority shall see that they are kept in a manner that protects



their confidentiality whilst guaranteeing the right of the parties to the proceedings to view them without taking a copy.

9. Whoever unlawfully destroys a document belonging to the DIS or to the Security Intelligence Services at any stage of its declassification, or one no longer covered by any restriction after expiry of the time limits, shall be punished with imprisonment for a term of between one and five years.

## Chapter VI

### TRANSITIONAL AND FINAL PROVISIONS

#### Section 43

##### *(Procedure for adopting Regulations)*

1. Save where otherwise established, the regulatory measures provided for by this Act shall be adopted within one hundred and eighty days from the date this Act comes into force. They shall be adopted by way of one or more Decrees issued by the President of the Council of Ministers, (including in derogation from section 17 of Law no. 400 of 23 August 1988, as subsequently amended), after obtaining the opinion of the Parliamentary Committee referred to under section 30 and after prior consultation with the CISR.

2. The said Decrees shall establish the system by which they are to be publicized. Such system may derogate from the laws in force.

#### Section 44

##### *(Laws repealed)*

1. Law no. 801 of 24 October 1977 is hereby repealed, save as provided for under subsection 2. With the exception of the provisions in implementing decrees concerning the legal protection of rights and interests in litigation involving staff retiring from the Security Intelligence Services, all the internal and regulatory measures that conflict with or are otherwise incompatible with this Act are likewise hereby repealed.

2. The CESIS, the SISMI and the SISDE shall continue to perform the tasks entrusted to them under Law no. 801 of 24 October 1977 until the date on which the Regulations referred to under section 4(7), section 6(10), section 7(10), section 21(1) and section 29(3) come into force.

3. The Regulations referred to under subsection 2 shall all come into force at the same time.

4. In all records having legal force, the term "SISMI" shall be understood as referring to the AISE, the term "SISDE" shall be understood as referring to the AISI, the term "CESIS" shall be understood as referring to the "DIS", the term "CIIS" shall be understood as referring to the CISR and references to the Parliamentary Oversight Committee are to be understood as referring to the Committee provided for under section 30 of this Act.

## Section 45

### *(Transitional Provisions)*

1. Within ten days of this Act's entry into force, the Interministerial Committee for the Security of the Republic shall be established and the Parliamentary Committee referred to under section 11 of Law no. 801 of 24 October 1977 and established during the XV Parliament, shall undergo an integration of its membership, pursuant to section 30(1) of this Act. The Interministerial Committee for Intelligence and Security referred to under section 2 of Law no. 801 of 24 October 1977 shall cease to carry out its functions with effect from the same date.
2. Even during its first stages, the implementation of this Act shall be effected without exceeding the limits for human, material and financial resources already set by legislation currently in force. To such end, the funds already officially set aside for analogous requirements in the Ministry of Economy and Finance's estimate shall be incorporated in the basic allocation referred to under section 29(1). The Minister of Economy and Finance shall be authorized to effect necessary budget variations by way of Decree.
3. The rules referred to under section 28 shall apply to evidence acquired after the date this Act comes into force.

## Section 46

### *(Entry into Force)*

1. This Act shall come into force on the sixtieth day after the date of its publication in the *Official Journal*.