Strasbourg, 2 February 2023 **CDL-REF(2023)002**

Opinion No. 1117 / 2022 Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW

(VENICE COMMISSION)

REPUBLIC OF MOLDOVA

DRAFT LAW

ON COUNTERINTELLIGENCE AND EXTERNAL INTELLIGENCE ACTIVITY

Law
on counterintelligence and external intelligence activity

Parliament adopts this Organic Law

Chapter I
GENERAL

Article 1. Notions, purpose and regulatory area

(1) This Law lays down the legal framework for the counterintelligence and external intelligence activities *(hereinafter – intelligence/counterintelligence*) carried out by the Intelligence and Security Service of the Republic of Moldova (*hereinafter – the Service*), the manner and conditions for ordering and carrying out counterintelligence measures and external intelligence measures, and for reviewing their legality**.**

(2) Counterintelligence activity consists of all the measures, actions, operations and processes carried out by the Service in order to protect the political and state decision-making process, protect the state and society institutions from risks and threats to the security of the Republic of Moldova, identify the intentions, plans and objectives of subversive activity, espionage or organised crime endangering state security, prevent, counteract or neutralise their materialisation, study the organisation, methods, capabilities and characteristics of the adverse party, followed by detection, prevention and counteraction.

(3) External intelligence activity shall consist of all measures, actions and operations carried out by the Service for the planning, collection, verification, analytical processing and exploitation of data and information about actual or potential possibilities, actions, plans or intentions of foreign States or organisations, unconstitutional entities or individuals, which constitute or could pose risks or threats to the security of the Republic of Moldova, and to obtain information relevant to the provision of state security or the creation of conditions conducive to ensuring and promoting strategic interests and the successful implementation of the Republic of Moldova's national security policy.

Article 2. Principles of intelligence/counterintelligence

The intelligence/counterintelligence activity is based on the principles of:

a) legality;

b) equality before the law for all;

c) respect of human rights and freedoms and regulate exclusively by law the limitation of their exercise;

d) opportunity;

e) proportionality;

f) the active nature of the measures carried out;

g) confidentiality, the combination of methods and means of public and secret activity;

h) political neutrality and impartiality.

Article 3. Ensuring the legality of the intelligence/counterintelligence activity

(1) The lawfulness of the intelligence/counterintelligence activity shall be ensured by carrying out control of this activity in accordance with the provisions of this Law.

(2) The carrying out of intelligence/counterintelligence activities for purposes other than those referred to in this Law shall not be permitted.

(3) Carrying out the intelligence/counterintelligence activity in breach of this Law shall give rise to the liability provided for in the legislation.

Article 4. Subjects carrying out the intelligence/counterintelligence activity

(1) The intelligence/counterintelligence work is carried out by the Service through the Intelligence and Security Officers *(hereafter – intelligence officers*) of its specialised subdivisions.

(2) Authorities or persons other than those referred to in this Article shall not be entitled to carry out the intelligence/counterintelligence activity.

Article 5. Rights of the subjects carrying out the intelligence/counterintelligence activity

(1) In carrying out the intelligence/counterintelligence activity, the Service and the intelligence officers have the rights set out in the Law on the Intelligence and Security Service of the Republic of Moldova and Law No 170/2007 on the status of the intelligence and security officer.

(2) When carrying out the intelligence/counterintelligence activity, intelligence officers shall have the right to:

a) to capture photos, make audio and video recordings without violating the inviolability of the individual's privacy;

b) communicate directly, including legend, with persons possessing information about facts, events, circumstances, or persons, with or without the recording of the discussion using technical means;

c) carry out testing using polygraph in accordance with the procedure established by Law No 269/2008 on the application of testing to simulated behaviour detector (polygraph)

d) to directly study documents, materials, information systems, databases, including through the interoperability platform, to make requests to legal and natural persons who possess or possess information in order to obtain information about natural or legal persons, goods, facts, events, circumstances. The service shall establish the rules and keep records of access to databases;

e) identify the person after static alerts (papillary prints, saliva and blood composition, DNA, odour traces, other traces left) and dynamic (walking, gesticulating, mimics, etc.), as well as by means of the photoroboty and other methods that make it possible, with a higher probability, to identify the person.

(3) In order to carry out the intelligence/counterintelligence activity, the Service shall have the right to:

a) to acquire, create, maintain, refine, manage information systems and electronic communications networks on their own technological platforms;

b) set up and manage databanks in which information relevant to ensuring State security is included;

c) to produce and use documents, documents, stamps or other items for encoding the identity of natural and legal persons, specialised subdivisions, rooms and means of transport.

(4) In carrying out the intelligence/counterintelligence activity, the Service shall be given access free of charge to the information systems of bodies protecting the rules of law, public authorities, centres, businesses, institutions and organisations, irrespective of the type of ownership.

Article 6. Persons collaborating confidentially with the Service

(1) Persons who collaborate confidentially with the Service are individuals who, by written or oral agreement, have given their consent to provide confidential information to the Service, to participate confidentially in the preparation and performance of the intelligence/counterintelligence activity, and to contribute in another way, not prohibited by law, to the intelligence/counterintelligence activity.

(2) The agreement shall be concluded between the intelligence officer on behalf of the Service and the individual.

(3) Support to the Service may be free of charge or remunerated.

(4) Persons collaborating confidentially with the Service have the rights and obligations set out in Law No 619 of 31 October 1995 on State Security Authorities and the Law on the Intelligence and Security Service of the Republic of Moldova.

(5) In order to ensure the security of persons who cooperate confidentially with the Service, their family members and relatives, intelligence/counterintelligence measures may be carried out in order to protect them in the manner laid down by law.

(6) Information about persons who cooperate confidentially with the Service shall constitute a state secret and may be declassified in accordance with the procedure laid down in Law No 245/2008 on State secrecy and only with the person's written consent.

(7) The activity of persons working confidentially with the Service is under the control of the head of the unit carrying out the intelligence/counterintelligence activity and is subject to internal control.

(8) In the event of the death of a person who has consented in writing to collaborate confidentially with the Service, in direct connection with his participation in the preparation and/or performance of the intelligence/counterintelligence activity, the members of the deceased's family and the persons maintained by him shall be paid, in equal shares, by means of the State budget, a one-off allowance of 120 average monthly salaries per economy.

(9) In the event of mutilation (injury, trauma, contusions) of a person who has consented in writing to collaborate confidentially with the Service, in direct connection with his participation in the preparation and/or carrying out of the intelligence/counterintelligence activity, which has led to severe, severe or average disability, and which deprives him of the possibility of continuing to cooperate, he shall be paid, from the resources of the State budget, a one-off allowance of 60, 50 or 40 average monthly salary per month per economy corresponding to the degree of disability received.

Article 7. Assistance in carrying out the intelligence/counterintelligence activity

(1) Individuals and legal entities irrespective of the form of ownership, shall be required, in accordance with this Law, to provide the necessary assistance to the Service, to make the requested information immediately and free of charge available to it, as well as, as far as possible, movable and immovable property, other objects and documents necessary for carrying out the intelligence/counterintelligence activity.

(2) Postal service providers and providers of electronic communications networks and/or services, irrespective of the type of ownership required:

1) to provide premises, equipment and technical conditions necessary for the Service to carry out external counterintelligence or intelligence measures and, to that end, to present the necessary technical data;

2) take action to preserve the confidentiality of the content, methods and tactics of external counterintelligence or intelligence measures;

3) ensure that the conditions of the general authorisation, the rules for interconnection of networks and access to electronic communications networks and/or services, as well as the requirements laid down by the National Regulatory Agency for Electronic Communications and Information Technology in coordination with the Service, are met in relation to electronic communications networks and the associated infrastructure for carrying out external counterintelligence or intelligence measures;

4) to ensure unrestricted and operational access by the specialised subdivision of the Service to all interfaces of providers' equipment, to their own electronic communications networks, to provide the necessary technical conditions and data for connecting the special pre-designed technical means to carry out external counterintelligence or intelligence measures;

5) to ensure at all times and continuously the technical conditions necessary for the connection and operation of special technical means designed to carry out external counterintelligence or intelligence measures in full volume and real-time, in particular as regards:

a) compliance of the supplier's equipment specification with the format accepted by the special technical means;

b) the supplier's willingness to connect special technical facilities via fixed connections or through a switch;

6) provide technical support to the Service in carrying out its tasks in the field and cooperate with it in implementing the criteria for securing and auditing the national interception system;

7) make available to the Interception Management Servers Service and the administration and operation consoles they hold, in order to ensure the function of lawful interception of communications;

8) ensure that special technical means installed in suppliers' rooms are protected against information theft or unsanctioned access, under the conditions laid down for the

protection of suppliers' equipment. Access to these rooms shall be restricted to the responsible intelligence officers specifically designated for that purpose by the Director of the Service;

9) to ensure continuous access of the Service to subscriber databases (which will be required to contain technical identifiers and subscribers' identity data, if known), by linking the Service's technical means to the equipment of providers of electronic communications networks and/or services, or by other mutually agreed methods, for the purpose of carrying out counterintelligence measures in accordance with the law;

10) inform the Service in advance of any network change that may affect the continuity of external counterintelligence or intelligence measures in electronic communications networks;

11) upgrade and/or expand their electronic communications networks and associated facilities in such a way as not to impair the continuity of carrying out external counterintelligence or intelligence measures in electronic communications networks. Where the upgrading and/or extension of the electronic communications network or associated infrastructure may prevent external counterintelligence or intelligence measures from being carried out, their entry into service shall take place at the same time as the installation on the provider's account of the additional equipment necessary to connect the special technical means and adjust the format for the transmission of information to the format accepted by the special technical means.

(3) Central government bodies, subdivisions and institutions subordinate to them are obliged, upon request, to make available to the Service functions to which intelligence officers will be seconded for intelligence/counterintelligence purposes.

Article 8. Use of technical means to carry out the intelligence/counter intelligence activity

In carrying out the intelligence/counterintelligence activity, the use of informational databases, special technical means for hiding the information, video, audio or other technical means shall be permitted.

Article 9. Special file

(1) In order to collect and systematize the information, to check and assess the results of the intelligence/counterintelligence activity and to take the appropriate decisions on the basis thereof, special files shall be initiated in which all the material accumulated is attached. The initiation of the file is subject to compulsory registration.

(2) Each special file shall include a mechanism for record-keeping of persons who have made themselves aware of the file materials, which shall include:

a) surname, first name and position of the person;

b) the date, year and time of the initiation of knowledge of the file materials and the date, year and time of its completion;

c) information relating to access to the entire special file, certain documents or compartments thereof,

d) signature of the person.

(3) The service shall ensure the necessary measures to protect the information held in the special files of disclosure, modification or destruction. In cases where the information held in the Special Files of the Service is no longer necessary for the performance of its tasks or where there is any other legal basis, the Service will destroy or retain it in such a way as to allow access only in cases exclusively regulated by law.

(4) The initiation of the special file cannot serve as a basis for limiting the human rights and freedoms provided for by law.

Article 10. Management of materials not relevant to the intelligence activity/counterintelligence

Once the investigation of the case has been completed, as part of the intelligence/counterintelligence activity, and the closure of the special file, the material which has proved to be irrelevant to the case under investigation is destroyed, with the exception of documents confirming the authorisation and implementation of a counterintelligence measure or other exceptions provided for by law, with the preparation of an act to that effect. The rest

of the material shall be archived and shall follow the arrangements for the retention of the special file, with subsequent destruction or, where appropriate, declassification and transfer to the National Archive of the Republic of Moldova, in accordance with the legal provisions.

Article 11. Departmental regulation of intelligence/counterintelligence

The organisation and as well the methods for carrying out external counterintelligence or intelligence measures, internal authorisation procedures, rules for drafting protocols of retention and destruction of materials obtained, measures to ensure their integrity and confidentiality and intelligence/counterintelligence activities, rules for carrying out undercover operations, how to register special files, their category, starting, managing, terminating, the time limits for their retention and the procedure for their adjustment, as well as the use of the financial resources allocated to carry out external counterintelligence or intelligence measures, the methods of working with persons cooperating confidentially with the Service, including the way in which the information submitted by them is documented, the categories of such persons, the organisation, forces, means, sources, methods, plans, procedures and tactics of carrying out the intelligence/counterintelligence activity, and the use of the results thereof, constitute state secret information and are regulated by departmental legislative acts of the Service.

Chapter II
THE COUNTERINTELLIGENCE MEASURES

Section I
Procedure for authorising counterintelligence measures

Article 12. Counterintelligence measures

(1) The following counterintelligence measures may be carried out as part of the counterintelligence activity:

1) with the authorization of the Director of the Service or the Special Deputy Director empowered to:

a) access to financial information or monitoring of financial transactions;

b) identification of the subscriber, owner or user of an electronic communications system or an access point to an information system with or without the input of electronic communications service providers;

c) visual tracking and/or documentation by technical methods and means as well as tracking or tracking through the global positioning system or other technical means;

d) control of the transmission of money or other tangible or intangible values and the provision of services;

e) undercover investigation;

f) controlled delivery;

g) collection of samples for comparative research;

h) research of objects and acts;

i) acquisition of control;

j) investigating rooms, buildings, parts of land or means of transport, if this does not constitute a breach of home;

k) the operational experiment;

2) with a judicial warrant:

a) home investigation and/or installing, where appropriate, audio, video, photographic or fact-finding devices, with or without recordings;

b) home monitoring by using technical means with or without recording;

c) intercept communications with or without recording;

d) access to and/or follow-up of information found or processed in an information system with or without recording;

e) collection of information from providers of electronic communications services;

f) the detention, investigation, handover, search or clearance of postal items;

g) visual tracking with audio recording of the content of communications transmitted by persons in open spaces, public places or non-home rooms;

h) blocking of an access point connected to an information system or electronic communications networks;

i) operational experiment.

(2) The list of measures listed in paragraph (1) of this Article shall be exhaustive and may be amended or supplemented only by law.

Article 13. Grounds for carrying out counterintelligence measures

(1) The grounds for carrying out counterintelligence measures include:

1) information that has become known, concerning:

a) conduct in the course of preparation, commission or commission which endangers the security of the State, as well as persons who prepare, commit or have committed it, their accomplices;

b) circumstances endangering the security of the covert investigator, intelligence officer, persons collaborating confidentially with the Service or members of their families;

c) potential state security risks and threats;

2) research into or counteract the activity of special services of foreign states or unconstitutional entities;

3) interpellations of international organisations or of the law enforcement authorities of other States, in accordance with international treaties to which the Republic of Moldova is a party or on the basis of collaboration agreements between the Service and the relevant public authorities of other States;

4) interpellations of the authorities which organise and carry out the special investigation, prosecution, trial of cases, in the event of acts endangering the security of the State;

5) the need to obtain information in the interest of ensuring the security of the Republic of Moldova, enhancing its economic, technical and scientific potential or defensive, creating the conditions for the promotion of its foreign and internal policy;

6) the protection of state secret;

7) collection of the necessary information characterising the persons subject to verification on:

a) access to information that is secret by the State;

b) admission to work for critical infrastructure objectives;

c) admission to the organisation and implementation of external counterintelligence and/or intelligence measures or access to materials received in the course of carrying out such measures;

d) establishing or maintaining working relationships in the organisation and conduct of external counterintelligence or intelligence measures;

8) screening of candidates or holders of public office;

9) ensuring internal security.

Article 14. Procedure for the authorisation of counterintelligence measures by the Director of the Service or the Deputy Director specifically empowered

(1) The counterintelligence measures referred to in Article 12 paragraph (1) point 1) of this Law shall be authorised, by order, by the Director of the Service or the specially empowered Deputy Director, at the request of the head of the subdivision carrying out the intelligence/counterintelligence activity in a special file opened and registered.

(2) This will include: the factual circumstances which serve as a basis for carrying out counterintelligence measures; where appropriate, their possible consequences; the motivated reasons for carrying out those measures specifically; the number of the special file in which the measures are to be carried out; the expected results of these measures; the time limit for carrying out those measures; if an extension of the measure is requested, the dates of the previous authorisations and the cumulative deadline for carrying out the measure shall be indicated; place of performance; the identification of the person subject to the measure, if known; other relevant data.

(3) The Order of the Director of the Service or the Deputy Director specifically empowered shall include:

a) the date of completion;

b) the particulars of the special file in which the measure is authorised;

c) the specific measure authorised;

d) the period for which it has been authorised, if any;

e) the subdivision of the Service or, as the case may be, the intelligence officers, who will carry it out, if the measure is not carried out directly by the intelligence officer who submitted the action;

f) other information, if provided for in this Act.

(4) The Director of the Service, the Deputy Director specifically empowered, will refuse to authorise the counterintelligence measure if he finds that the action put forward is unfounded and unsubstantiated.

Article 15. Procedure for authorising counterintelligence measures by issuing a court warrant

(1) The court warrant is the authorisation to carry out, in a special open and registered file, the counterintelligence measures constituting an interference with private life, as referred to in Article 12 paragraph (1), point 2) of this Law.

(2) The court warrant shall be issued, at the written request of the Director of the Service or the Special Deputy Director, by a judge of the Chisinau District Court specifically empowered to do so.

(3) The counterintelligence measure referred to in Article 12 paragraph (1) point 2).a) of this Law shall be authorised on the basis of the written action of the Director of the Service or the Special Deputy Director, coordinated in advance with a special prosecutor appointed from the General Prosecutor's Office, and only if other counterintelligence measures previously carried out have not achieved the intended purpose.

(4) The judge, prior to the power of issuing court orders, will obtain according to law, the right of access to state secret, if at the moment he does not have such a right.

(5) The process for issuing the court warrant contains the following data:

a) the surname, first name and position of the person applying for the issue of the warrant;

b) the identification data of the person subject to the counterintelligence measure, if known;

c) the counterintelligence measure for which authorisation is sought;

d) the factual circumstances which serve as the basis for carrying out the counterintelligence measure and, where appropriate, their possible consequences;

e) in the case of a request for an extension of the time limit for carrying out the measure, the circumstances justifying the extension;

f) the expected results of the counterintelligence measure;

g) the time limit for carrying out that measure;

h) the place where the counterintelligence measure was carried out;

i) other data relevant to the justification of the counterintelligence measure and which would guarantee its lawful and well-founded authorisation.

(6) The examination of the request of the court warrant takes place during the day on which it was submitted, at a closed hearing, with the participation of the intelligence officer, who will give the necessary explanations. In the course of examining the matter, the judge may be presented with material confirming the need to carry out those measures, without those measures being annexed to the request and without disclosing the identity of the persons who collaborate confidentially with the Service.

(7) In order to issue the court warrant, the judge shall further verify that:

a) the discovery of the circumstances of the case is impossible or excessively difficult by other counterintelligence measures, or the danger to the security of the person concerned persists, or there is a high likelihood of deconspiration of other counterintelligence measures;

b) the requested action pursues a legitimate aim;

c) the action will be proportionate to the right or freedom of the person guaranteed by law and the need arising.

(8) After carrying out a review of the merits of the action, the judge, by concluding a decision, issues a court warrant or rejects the action.

(9) The conclusion shall be drawn up and matured immediately, but no later than 24 hours after it has been delivered. In cases of urgent urgency, the judge shall, upon request, issue the operative part of the conclusion, with subsequent production, within the prescribed period, of the reasoned conclusion.

(10) The judge's conclusion on the issue of the court warrant contains the following data: the date and place of completion of the conclusion; the name and first name of the judge; the surname, first name and position of the person applying for the issue of the warrant; the body carrying out the counterintelligence measure; the identification data of the person subject to the counterintelligence measure, if known; the data justifying the need to carry out and authorise the counterintelligence measure, respectively; authorised counterintelligence measures; the time limit for carrying out the counterintelligence measure; the place where the counterintelligence measure is to be carried out; other data that are important for justifying the authorisation of the counterintelligence measure.

(11) Counterintelligence measures, which can only be carried out with a court warrant, may, by way of exception, be carried out, without this, on the basis of a reasoned decision of the Director of the Service or the Deputy Director specifically empowered, where there are exceptional circumstances which do not allow for delay and the court warrant cannot be obtained without the existence of a substantial risk of delay which may lead to the loss of relevant information or immediately jeopardise the security of the State or of persons. In this case, the judge is to be informed within 24 hours from the order of the measure that it has been carried out, providing him with all the material in which the need to carry out the counterintelligence measure is substantiated and the circumstances which have not allowed it to be remembered. If there are sufficient grounds, the judge confirms, by means of a reasoned decision, the lawfulness of carrying out the measure. Otherwise, the judge declares the measure to be unlawful.

(12) Counterintelligence measures initiated pursuant to paragraph (10) of this Article shall be carried out until the judge's conclusion is issued, but not more than 24 hours after they have been initiated, and shall then proceed in accordance with the provisions of the judge's conclusion.

(13) At the same time as declaring the measures to be lawful, the judge, upon request, issues a court warrant to continue to carry them out.

(14) When declaring the measures to be illegal, the judge orders the destruction of the information gathered through this measure. The destruction of the information shall be carried out by the Service within 15 working days, with a report to that effect being drawn up, an authenticated copy of which shall be submitted to the judge. At the same time, the judge informs the Prosecutor General to verify that the actions of the intelligence officers do not contain the constituent elements of the offence.

(15) The reasoned conclusion of the judge on the rejection of the court warrant, as well as the reasoned conclusion on declaring the measure illegal and ordering the destruction of the information gathered, may be challenged by the Service with an appeal to the Criminal College of the Chisinau Court of Appeal. The appeal shall suspend the action to destroy the information.

(16) The appeal shall be examined by a panel of three judges in accordance with paragraphs (5) and (6) of this Article. The judges of the appeal panel shall be specifically designated for this purpose and shall proceed with the procedure laid down in paragraph (3) of this Article.

(17) The appeal shall be lodged within 3 working days from the date of receipt of the reasoned order and shall contain the factual and legal grounds of illegality and/or illegality of the decision.

(18) After examining the appeal, the formation of the Criminal College of the Curtea de Apel Chisinau (Court of Appeal, Chisinau), by decision:

a) admit the appeal, quash the decision and, where appropriate, issue a court warrant or declare the measures to be lawful;

b) dismisses the appeal and upholds the form of order sought;

(19) The decision shall be drawn up in accordance with the provisions of paragraph (8) of this Article.

Article 16. Special conditions for carrying out counterintelligence measures authorised by the issuing of the court warrant

(1) The counterintelligence measures referred to in Article 12 paragraph (1), point 2) of this Law shall be ordered to investigate the following facts which present a particular danger to the security of the State:

a) actions aimed at violently changing constitutional order, undermining or liquidating the sovereignty, independence or territorial integrity of the country;

b) activity contributing, directly or indirectly, to military action against the country or to the triggering of the civil war;

c) military or other violent actions undermining the foundations of the state;

d) actions aimed at violently overthrowing the legally elected public authorities;

e) actions that foster the emergence of exceptional situations in transport, electronic communications, to the objectives of critical infrastructure;

f) state treason, espionage, illegal intelligence activity, conspiracy against the Republic of Moldova, unauthorised intelligence gathering;

g) attacks on the life, health or inviolability of dignitaries of the Republic of Moldova and foreign dignitaries, their family members benefiting from state protection;

h) the removal of arms, ammunition, combat techniques, explosives, radioactive substances, poisoners, narcotic substances, toxic and other substances, their smuggling, their illegal production, use, transport and storage, if this is detrimental to the interests of state security;

i) the constitution of, or participation in, the activity of illegal entities, organisations or groups endangering the security of the State;

j) terrorist activities, the financing or material insurance of terrorist acts.

(2) The counterintelligence measures referred to in Article 12 par. (1) point 2) of this Law shall be ordered with regard to:

a) the person in respect of whom there is a documented reasonable suspicion that he or she is preparing, undertaking attempts to commit or has committed one or more of the acts referred to in paragraph (1) of this Article;

b) a person who is reasonably suspected of receiving or transmitting communications or objects from, or intended for, the persons referred to in point (a) of this paragraph;

c) to persons other than those referred to in points a) and b) of this paragraph, if there are reasonable grounds to suspect that the means of communication, their place of residence or their property are used by the persons referred to in points (a) and/or (b) of this paragraph for the purposes referred to in point (a).

(3) Counterintelligence measures referred to Article 12 par. (1) point (2) of this Law may be taken with regard to persons who contribute to the carrying out of the intelligence/counterintelligence activity, as well as their relatives and family members, only with the written consent or at their express and prior written request and if there is an imminent danger to their life, health or other fundamental rights, or if it is necessary to prevent the crime or adverse consequences for those persons.

Article 17. Period for which counterintelligence measures are authorised

(1) The counterintelligence measures referred to in Article 12 par. (1) point 1), which do not constitute one-off measures, with the exception of those referred to in points e) and f), shall be authorised, for a period of up to 90 days, with the possibility of extension for successive periods and for non-successive periods of up to 90 days.

(2) Counterintelligence measures, as referred to in Article 12 par. (1) point 2), which do not constitute one-off measures, with the exception of those referred to in points a) and h), shall be authorised for a period of up to 90 days, with the possibility of extension for successive periods and for non-successive periods of up to 90 days.

(3) The counterintelligence measures referred to in Article 12 par. (1) point 1).e), f) and point. 2).h) shall be authorised for a period of up to 6 months, with the possibility of extension for successive periods and for non-successive periods up to 6 months.

(4) The counterintelligence measures referred to in Article 12 par.(1) point. 2).a) shall be authorised for a period of up to 30 days, with the possibility of extension for successive periods and for non-successive periods of up to 30 days.

(5) The total duration of the special investigative measure in respect of a person ordered in respect of a specific act may not exceed 2 years cumulatively. At each request for an extension of the time limit for carrying out the special investigative measure, the judge shall be required to examine the circumstances justifying such an extension and, if he considers that the request is not reasoned, refuse the extension.

(6) Counterintelligence measures must begin on the date indicated in the instrument of disposal or on the date of expiry of the period for which it was authorised.

Article 18. Reporting the results of the counterintelligence measure

The intelligence officer, who carries out/initiates the counterintelligence measure, shall inform the Director of the Service or the Special Deputy Director authorised by means of a report, within one month of the date on which the measure was completed, or within the time limit laid down in the instrument of disposal, of the results obtained in implementing the authorised measure.

Article 19. Termination of the counterintelligence measure before the deadline

(1) The Director of the Service or the specially empowered Deputy Director shall terminate the counterintelligence measure before the expiry of the period for which it was authorised, or for which a court warrant has been issued, as soon as the grounds and reasons justifying its authorisation have disappeared.

(2) If the necessary grounds for carrying out the counterintelligence measures no longer exist, the intelligence officer shall, with the agreement of the Director of the Service or the Deputy Director specially empowered, cease to conduct it. If a court warrant has been issued to carry out the counterintelligence measure, the grounds for and the early termination of the measure shall be informed of the judge who issued the judicial warrant.

Article 20. Record of counterintelligence measures

(1) The intelligence officer carrying out the counterintelligence measure shall draw up a report for each authorised measure in which he shall record:

a) the name of the counterintelligence measure carried out, the place and date on which it was carried out, as the case may be, the time of its commencement and completion, details of the authorisation of the measure or the judicial warrant;

b) position, surname and first name of the information officer who draws up the report. If the counterintelligence measure has been carried out directly by the intelligence officers from within the assurance subdivision of the intelligence/counterintelligence, who are part of the Service's cryptic staff, the report shall indicate the position, surname and first name of the head of the given subdivision, who shall verify the correctness of the details mentioned in the minutes and sign it. Within those subdivisions, strict records shall be kept of the intelligence officers who have carried out counterintelligence measures and have drawn up minutes;

c) the names, forenames and status of the persons who participated in the execution of the measures and, if necessary, their addresses, objections and explanations. Such data shall not be recorded in the minutes in the event of the participation in the measures of the intelligence officers of the intelligence/counterintelligence assurance subdivision, who are part of the Service's cryptotic staff;

d) description of the facts found and of the actions taken in carrying out the counterintelligence measure;

e) an indication of the use of the technical means, the conditions and procedures for their application, the objects to which those means have been applied, the results obtained, and the recording of the information gathered.

(2) If the results of the counterintelligence measure are recorded, the physical information carrier shall be attached to the report.

(3) The report and the material carrier of the information shall be attached to the special file.

Article 21. Use of the results of counterintelligence measures

(1) The results of counterintelligence measures shall be used:

a) in carrying out the tasks of the Service;

b) when carrying out other counterintelligence measures;

c) when carrying out special investigative measures, for the purpose of detecting, preventing, curbing crime and ensuring public order.

(2) Information about the forces, means, sources, methods, plans and results of the intelligence/counterintelligence activity, as well as the organisation and tactical conduct of counterintelligence measures, shall be secret by the State and may be declassified only in accordance with the law.

(3) If, after the counterintelligence measures have been carried out, a reasonable suspicion is found that a crime has been committed or that it has been prepared to commit it, a report shall inform the special prosecutor of the General Prosecutor's Office.

(4) The results of counterintelligence measures in a special file may be used in another special file only with the authorisation of the judge or, where applicable, the Director of the Special Authorised Deputy Service/Director, who has issued a judicial warrant, or, where appropriate, the Order, to carry out those counterintelligence measures.

(5) The results of counterintelligence measures cannot constitute evidence in a criminal case.

Article 22. Confidentiality of data on counterintelligence measures

(1) Information on the carrying out of counterintelligence measures, as well as the results of such measures, shall constitute state secret information.

(2) Persons who are aware, by virtue of their function, of their quality, of circumstances, or of the performance of counterintelligence measures, or of the results thereof, must be kept confidential.

(3) Any unauthorised disclosure of the information referred to in paragraph (1) shall give rise to the liability provided for by the legislation in force.

Article 23. Informing the person of counterintelligence measures taken against him or her

(1) Once the investigation of the case has been completed and the special case has been closed**,** if the counterintelligence measures referred to in Article 12 par. (1) point 2) have been carried out, within 5 working days of the closing date, the Service shall inform the persons in respect of whom those measures have been carried out. The material confirming that the person has been informed shall be attached to the special file.

(2) In each case of informing the persons in respect of whom the counterintelligence measures referred to in Article 12 par. (1) point 2) have been carried out, the Service shall notify the judge who issued the court warrant thereof.

(3) The person shall not be informed if there are reasonable grounds to believe that this could constitute an increased risk to human life or health, jeopardise another investigation conducted, harm the security of the State or prejudice the purpose for which the counterintelligence measures were carried out.

(4) On the existence of the grounds referred to in paragraph (3), the intelligence officer, who carried out the investigation of the case, shall draw up a written report detailing those grounds and submitting it for approval to the Director of the Service. If the report is approved, the Director of the Service shall ask the judge who issued the judicial warrant for authorisation not to inform the person.

(5) The judge, when examining the action taken by the Director of the Service, shall find that there are no or no grounds for not informing the person, shall determine whether those grounds are permanent or provisional, and, where appropriate, shall accept or refuse authorisation not to inform the person. Depending on whether the grounds for non-information are permanent or provisional, the judge may authorise permanent non-information or non-information for a specified period of time, but no longer than 1 year, the Service being obliged upon expiry of that period to reassess the grounds for non-information and to take the necessary action, in accordance with the provisions of this Article, including, where appropriate, requesting the person not to be informed for a further period of time. A refusal to

authorise non-information may be challenged by the Appeals Service, and the provisions of Article 15 of this Law shall apply accordingly.

(6) If the grounds for failure to inform the person subject to the counterintelligence measure have disappeared in advance, the investigation officer shall draw up a report and submit it for approval to the Director of the Service requesting that the person be immediately informed. If the report is approved, the person shall be informed in accordance with paragraph (1) of this Article.

(7) The conclusion of the judge authorising failure to inform and the approved report shall be attached to the special file.

Section II
Definition of counterintelligence measures

Article 24. Access to financial information or monitoring of financial transactions

(1) Access to financial information is the obtaining from banks, financial institutions, other persons/organisations acting as intermediary in financial transactions or other competent institutions, of documents or information in their possession relating to deposits, accounts or transactions of a person, or the circulation of a certain sum of money.

(2) Monitoring of financial transactions means operations which ensure knowledge, including real-time knowledge, of the content of financial transactions carried out through banks, financial institutions, other persons/organisations intermediating financial transactions or other competent institutions relating to deposits, accounts or transactions of a person, or the movement of a certain sum of money.

(3) Banks, financial institutions, other persons/organisations involved in financial transactions or other competent institutions shall be presented with the extract of the Order of the Director of the Service or Deputy Director with special authority, indicating only the category of information to be submitted and, where appropriate, the time limit for carrying out the monitoring.

Article 25. Identification of the subscriber, owner or user of an electronic communications system or an access point to an information system with or without the input of electronic communications service providers

(1) The identification of the subscriber, owner or user of an electronic communications system or of an access point to an information system shall consist of establishing, with or without the input of an electronic service provider, the identity of the subscriber, owner or user of an electronic communications system, a means of electronic communications or an access point to an information system, or determining whether a particular communication means or access point to an information system is used or active, or has been used or active on a given date, or the determination of the means of electronic communications present at a given time at a person.

(2) Service providers are required to collaborate with the Service and to make immediately available to them the data requested on the basis of the extract from the Order of the Director of the Service or the Deputy Director specifically empowered, indicating only the category of information to be submitted.

(3) If the counterintelligence measure is carried out with the assistance of an electronic service provider, that provider shall, after receiving the extract from the Order of the Director of the Service or the Deputy Director specifically empowered to authorise the measure, submit the information requested without keeping the copy (including in electronic form) of the reply and the data sent, as soon as possible, but no later than 24 hours after receipt of the authorisation.

Article 26. Visual tracking and/or documentation by technical methods and means, and tracking or tracking through the global positioning system or other technical means

(1) Visual tracking and/or documentation using technical methods and means means the drawing up and fixing of buildings, premises, means of transport, actions/inactions

by the person, other factual circumstances occurring, with or without the use of technical recording equipment.

(2) Tracking or tracking through the global positioning system or other technical means consists of the use of devices to determine the whereabouts of the person or object, as well as the monitoring of their movement or intrusion directions, with or without recording of the acquired information.

Article 27. Control of the transmission of money or other tangible or intangible values and the provision of services

Control of the transmission of money or other tangible or intangible valuesand the provision of services is the supervision and documentation of the handover or handing over of money, other tangible or intangible securities or the provision of services to the person claiming, accepting, extorting or offering them, as well as by persons acting on their behalf or in their interest.

Article 28. Undercover investigation

(1) Undercover investigation shall consist of the infiltration of the covert investigator into a group of persons or the legalised initiation/maintenance of collaboration with a person in order to: gathering of information; ascertaining whether or not facts have been planned; the determination of people to dissuade themselves from deeds; the determination of persons to cooperate with the Department or bodies responsible for protecting the rules of law; disinformation; redirection of the activity; preventing certain actions from taking action; to prevent the negative consequences of wasted actions.

(2) The order ordering the undercover investigation shall contain in addition:

a) details of the person or persons to whom the undercover investigation will be conducted;

b) the identity attributed to the undercover investigator and the activities he/she will carry out;

c) details of the undercover investigator, where applicable, his name or the coded identity of the investigator.

(3) The undercover investigator may use technical means to record the facts in which he/she participates.

(4) Undercover investigators are designated intelligence officers or persons collaborating confidentially with the Service.

(5) The undercover investigator is prohibited from committing criminal offences.

(6) The service may use or place at the disposal of the undercover investigator any documents or objects necessary to carry out the measure.

Article 29. The activity of the undercover investigator and their protection measures

(1) In the process of the work carried out, the undercover investigator shall take action according to the situation created, in accordance with the personal conviction and guidance received from the Service.

(2) The identity of undercover investigators may be disclosed only with its written consent and in accordance with the Law on State Secret.

(3) If there is a real danger to the life and health of the undercover investigator, as well as in cases of discovery of his identity and quality, the Service shall immediately withdraw him from the covert investigation.

Article 30. Controlled delivery

(1) Controlled delivery means the movement under supervision of objects, goods or other valuables originating from activities which present a danger to the security of the State or are intended to carry out activities which pose a threat to State security, within the territory of the Republic of Moldova or across its borders, with the aim of preventing, countering, detecting, detecting or identifying persons who are involved in them.

(2) Controlled delivery, carried out across the borders of the Republic of Moldova, requires that, expressly, all States through which the goods referred to in paragraph (1) are transited:

a) consent to the entry into their territory of the said goods and their departure from the territory of the State;

b) ensure that the goods referred to, or the person transporting them or interacting with them, are kept under constant supervision by the competent authorities.

(3) The provisions of paragraph (2) of this Article shall not apply where a ratified international convention or an international agreement provides otherwise.

Article 31. Collection of samples for comparative research

(1) The collection of samples for comparative research shall consist of the detection, physical seizure and preservation of the material medium of information (objects, substances, etc.), for the purpose of comparing them with materials already available to the Service or for the subsequent detection of identical objects/substances to those of particular interest to the investigations carried out.

(2) The collection of samples in a way that endangers human health and life or adversely affects his honour and dignity shall be prohibited.

Article 32. Research of objects and acts

(1) Research on objects and acts consists of valuing the objects, acts, other documents and programme products from a scientific point of view in order to detect signs of activity posing a danger to the security of the State, to study their content, and to counteract them with other objects, documents, documents, programme products, necessary to determine the objective reality.

(2) The investigation of objects and acts shall be carried out by intelligence officers with the participation, where necessary, of the specialist with the necessary special knowledge.

Article 33. Acquisition of control

The acquisition of control shall consist of the purchase, whether for payment or not, of goods or services in free circulation, limited or prohibited, for the purpose of technical and scientific findings or for the investigation of activities posing a threat to the security of the Republic of Moldova or the identification of perpetrators who have committed or intend to carry out such activities.

Article 34. Investigation of rooms, buildings, parts of land or means of transport, if this does not constitute a breach of home

(1) Research into rooms, buildings, parts of land or means of transport, where this does not constitute a breach of home, involves access to them for the purpose of studying the traces of activity, persons of interest, in order to obtain other information necessary to establish the factual circumstances.

(2) Researching rooms, buildings, portions of land or means of transport, including with the use of special technical means, the intelligence officer shall examine them directly on them, examine objects in rooms, buildings, means of transport, on stretches of land, and examine other existing factual circumstances, identify their location and location, as appropriate, using special technical means, record the research process or certain objects or specific circumstances.

Article 35. Operational experiment

(1) The operational experiment shall consist of creating situations and circumstances characteristic of the daily work of the person subject to verification, for the purpose of detecting intent or recklessness and documenting his or her behaviour in those circumstances, if the information available shows a reasonable and reasoned assumption that:

a) the verified person prepares, undertakes attempts to commit or has committed an act which endangers State security, or;

b) this counterintelligence measure may curb the illegal activity of the person subject to verification, or;

c) as a result of the operational experiment, information about facts endangering State security may be obtained and without this counterintelligence measure it is impossible to obtain the necessary information or other measures applied will be disproportionate to their effectiveness.

(2) In the operational experiment, it is forbidden to provoke the actions of the person under examination, by promise or incitement, to influence him or her through violence, threats, blackmail, or to use his or her inability to determine when committing or continuing to commit an act.

(3) The act shall not be deemed to have occurred if it is evident from all the circumstances that the intelligence officer or the person collaborating confidentially with the Service has not done more (either through passive or active means) than to give the person the opportunity to commit an act that he or she would have used in the circumstances, in which he would have behaved in the same way if he had been given this opportunity by someone else.

(4) It is forbidden to carry out the operational experiment if it is likely to cause serious harm, endanger the life and health of its participants, state security.

(5) The Ordinance on the performance of the operational experiment shall contain in addition:

a) the data of the persons involved in carrying out the measure;

b) details of the person whose actions are to be fixed and documented (if identified), or, where appropriate, its characteristics;

c) specification of the actions to be taken.

Article 36. Home investigation and/or, where appropriate, installation in the home of audio, video, photographic, fact-finding devices, with or without recordings

(1) The search for the home and/or, where appropriate, the installation in the home of audio, video, photographic or fact-finding devices, with or without recordings, shall involve secret or legalised access within the home, without informing the owner, the possessor or the person living or residing in the home, for the purpose of studying him in order to discover the traces of activity, to persons of interest in order to obtain other information necessary to establish the factual circumstances, observe and record events occurring in the home. Where necessary, audio, video, photographic and fact-finding devices shall be installed in the home, which ensure that the information is intercepted and recorded remotely, or that it is recorded in the home with subsequent removal.

(2) By researching home, including with the use of special technical means, the intelligence officer shall examine home objects and other factual circumstances, identify their location and location, as appropriate, using special technical means, record the research process or specific objects or specific circumstances.

(3) In the context of the examination of residence, samples for comparative research may be collected if this does not lead to the deconstruction of the counterintelligence measure carried out.

(4) After the expiry of the authorisation period, or in the event of revocation of the home installation of devices providing audio, video, photographic surveillance or fact-finding equipment, secret or legalised home access shall be permitted, with the prior authorisation of the Director of the Service or the Special Assistant Director, for the removal of the apparatus in question. In the case of a given home, no other action than the removal of the device is investigated or taken. A report shall be drawn up of the entry into the home and the removal of the device, indicating the date and the persons who entered the home.

(5) The removal of the apparatus will take place within a more limited period after the end of the period for authorisation or revocation of the measure. It shall be prohibited to use in any way, including viewing or hearing, information recorded after the end of the authorisation period, or to revoke the measure, which shall be immediately destroyed.

Article 37. Home monitoring by using technical means with or without recording

The home monitoring by the use of technical means with or without recording shall involve the supervision of the external home, without the consent of the owner, the possessor or the person residing or located in the home, by the use of technical means, for the purpose of determining events occurring in that home, conversations, other sounds or factual situations, with or without recording those established.

Article 38. Interception of communications with or without recording

(1) Interception of communications means access, monitoring, collection of communications, transfer of data, information, with or without recording, by electronic communications networks or any other technical means of communication, as well as recording of traffic data indicating the source, destination, date, time, size, type of communication made, subscriber identification data or persons who made communications with the subject of the interception and their location or any other relevant information relating to the intercepted communication that may be established by technical means.

(2) The court order ordering the interception of communications must contain in addition the identification data of the subscriber or technical unit through which the communications to be intercepted are carried out, the actions authorised to be carried out as part of the interception of communications.

Article 39. Carrying out and certifying interception of communications

(1) The technical assurance of interception of communications shall be carried out by the specialised subdivision of the Service, using software products or special technical means connected, where necessary, to the equipment of the providers of electronic communications networks and/or services and/or of the subscriber. The intelligence officers of the subdivision responsible for the technical interception of communications, the employees who directly listen to the records, visualise the information communicated, translate them, draw up the verbatim report, shall keep the communications secret and shall be liable for failure to comply with this obligation.

(2) The information obtained in the process of intercepting communications can be listened to and viewed by the intelligence officer in real time.

(3) About the interception of communications, the intelligence officer who initiated the interception, within 24 hours after the expiry of the interception authorisation period, shall draw up a report at the end of each authorisation period.

(4) The interception record must contain the date, place and time of production, the position, the details of the intelligence officer who initiated the interception, the number of the special file in which the measure was carried out, the reference to the action taken by the Director of the Service or the Deputy Special Director and the judicial warrant issued; the identity and technical identification data of the subject whose communications have been intercepted and recorded, the period during which the communications were intercepted, the reference to the use of technical means, other relevant information obtained following the interception and recording of communications relating to the identification and/or location of subjects, the quantity and identification number of the media on which the information was recorded, the number of stenographic communications. The verbatim report of the communications relevant to the special file and the medium on which the intercepted communications were recorded shall be annexed to the minutes.

(5) The verbatim report constitutes the reproduction in writing of intercepted communications which are of importance for the special file. The verbatim report of communications shall indicate the date, time and duration of the communication, the names of the persons whose communications are to be stenographed, if known, and other data. The verbatim report shall be drawn up by the employees of the subdivision providing intelligence/counterintelligence and, if necessary or at the request of the intelligence officer who initiated the counterintelligence measure, personally by the latter.

(6) The intercepted communications shall be in the language in which the communication took place. If the communication took place in a language other than the State language, the communication shall be translated into the State language by a translator.

(7) The intelligence/counterintelligence assurance subdivision shall keep a hard record of the intelligence officers who had access to the intercepted communication, who drew up the verbatim report or translated the communication.

(8) Intercepted communications shall be fully retained on the initial medium presented by the specialised subdivision to the intelligence officer. This medium shall be kept secure in the special file. Access to that medium shall be subject to record being recorded:

a) the surname, first name of the person and position of the person who had access;

b) the date, year and time of the initiation of access and the date, year and time of completion of access;

c) whether the information recorded on the tangible medium has been heard/viewed;

d) the basis/reason for listening/viewing the information;

e) signature of the person.

Article 40. Access to information that is in or processed in an information system and/or its monitoring with or without recording

(1) Access to information which is located or processed in an information system requires that measures be taken to obtain information which is in an information system or is processed in an information system, or stored on a technical medium, with the possibility of recording the necessary information on a tangible medium.

(2) The monitoring of information contained in or processed in an information system requires measures to be taken in order to obtain in real time the actions taken in an information system, the information to be processed and the computer data associated with those actions.

(3) Access to and/or monitoring of information found in or processed in an information system may be carried out including:

a) by establishing a permanent or temporary physical link between the specialised subdivision of the Service and the equipment of the natural/legal person owning the information system or technical support;

b) through programme products;

c) by submitting directly to the holder of the information system the extract of the court warrant issued by the judge at the same time as the court warrant, indicating the category of information to be submitted.

Article 41. Collection of information from providers of electronic communications services

(1) The collection of information from providers of electronic communications services shall consist of collecting, with or without the assistance of providers of electronic communications services, information transmitted through technical communications channels, the secret fixation of information transmitted or received via technical communications links by persons subject to the counterintelligence measure, and obtaining from operators the information available, generated or processed in the course of providing their own electronic communications services, including roaming, necessary for the identification and tracing of the source of electronic communications, identification of the purpose, type, date, time and duration of the electronic communication, identification of the electronic communications equipment of the user or of another device used for communication, identification of the coordinates of mobile terminal equipment, and in particular:

1) the holders of telephone numbers (surname, forename, domicile);

2) telephone numbers registered in the name of a person;

3) electronic communications services provided to the user;

4) electronic communication source (technical identification data; surname, first name and domicile of the subscriber or registered user);

5) the destination of the electronic communication (technical identification of the caller; technical identification of the redirected access point, where applicable; surname, first name and domicile of the subscriber or registered user);

6) the type, date, time and duration of the electronic communication, including failed call attempts. Failed call attempt means the communication in which the call was successfully connected but not answered or an intervention related to network management took place;

7) the user's electronic communications equipment or other device used for communication purposes the IMSI and IMEI codes of the caller's and the caller's mobile phones; in the case of anonymous pre-paid services – the date and time at which the service was initially activated and the name of the location (Cell ID) from which the service was activated, as well as any data that may serve to identify the service user;

8) location of mobile communication equipment the location name (Cell ID) since the beginning of the communication; the geographical location of the cell by reference to the name of the location, during the period when the data are retained;

9) IP holders of static and dynamic addresses (surname, first name, domicile, business name, legal address, etc.) and the information identifying their communication equipment;

10) logs, generated or processed in the process of providing users of electronic communications services, necessary for the identification and tracing of the source of electronic communications, as well as other information traffic data.

(2) The collection of information from providers of electronic communications services shall be carried out:

a) by producing directly to the providers of electronic communications services the extract from the court warrant issued by the judge at the same time as the court warrant, indicating only the category of information to be submitted;

b) through the specialised subdivision of the service, using programme products or special technical means connected, where necessary, to suppliers' equipment.

Article 42. Detention, investigation, handover, search or clearance of postal items

(1) The detention, investigation, handover, search or clearance of postal items shall consist of the following actions taken without notifying the sender and the recipient of the postal items:

a) stopping the delivery of postal items for a strictly specified or relatively specific period of time, or delivering the postal item on a given date or time;

b) access and verification of postal items, visualisation of existing information, identification of objects or substances in the postal item;

c) failure to deliver the postal item and its takeover by the intelligence officer.

(2) Under the given measure, it is permitted to:

a) making the technical and scientific findings that will make it possible to identify the objects or substances in the postal consignment, or other factual situations;

b) copying, recording, using technical means, the information contained in the postal item.

(3) The judicial warrant concerning the detention, investigation, delivery, search or clearance of postal items must contain the name of the postal institution which is under the obligation to detain the postal items, the names and forenames of the person or persons whose postal items are to be detained, the exact address of such persons, if known or other characteristic elements on the basis of which the postal items may be identified, the kind of postal items against which the counterintelligence measure is directed.

(4) At the same time as the court warrant, the judge also issues an extract from it, which is sent to the head of the post office or postal item provider, for which enforcement of the measure set out in the extract is mandatory.

(5) The head of the post office or postal delivery provider shall immediately notify the information officer of the detention of the postal items indicated in the extract and shall ensure and preserve the confidentiality of the counterintelligence measure carried out.

Article 43. Visual tracking with audio recording of the content of communications transmitted by persons, in open spaces, public places or non-home rooms

Visual tracking with audio recording of the content of communications transmitted by persons, in open spaces, public places or non-home rooms, is the secret display and fixation,

including in electronic media, of the actions of one or more persons with the audio recording of the content of communications made by persons, if such actions take place in open spaces, public places or non-home rooms. In carrying out this measure, audio recording apparatus will be used, as necessary and video.

Article 44. Blocking of an access point connected to an information system or electronic communications networks

(1) The blocking of an access point connected to an information system or electronic communications networks shall entail the forced disconnection from an information system or electronic communications network of a means of communication with, or without, a prohibition on reconnection.

(2) The blocking of an access point connected to an information system or electronic communications networks shall be carried out by the Service using programme products, special technical means or electronic communications service providers upon presentation of the extract from the court warrant.

Article 45. Operational absconding

Operational absconding shall mean the secret removal, with the subsequent secret return, of the goods, documents and material media for their examination and analysis, the performance of the technical and scientific findings, the collection of the necessary information and the collection and analysis of samples.

CHAPTER III
EXTERNAL INTELLIGENCE ACTIVITY

Article 46. Tasks of external intelligence activity

The tasks of external intelligence activity are intended to:

1) detecting, preventing and countering external or external risks and threats to national security, mitigating or mitigating their consequences should they materialise, and protecting and promoting the strategic interests of the Republic of Moldova and its partners;

2) collecting, processing and ensuring the supreme leadership of the country and other authorities established by law, within the limits of their competence, with the information necessary for taking decisions and drawing up strategies in the spheres of national security, internal and external economic, energy, military, strategic, defensive, information, technical and scientific, humanitarian, environmental and protection of other national interests;

3) creating favourable conditions for national security and contributing to the formulation and implementation of foreign policy courses, development of the economy, technical and scientific progress, energy, information, environment and defence capacity of the Republic of Moldova;

4) ensuring the security of public authorities, institutions of the Republic of Moldova abroad and their employees, including external diplomatic missions and representations and their officials, members of their families, as well as citizens located outside the boundaries of the Republic, who have or have had access to information assigned to them by the state secret,

5) the regulation, coordination, conduct and control of state-secret information protection activities in missions and diplomatic representations of the Republic of Moldova abroad;

6) contributing to the identification, prevention and combating of international terrorism, actions against the sovereignty and integrity of the Republic of Moldova, other activities of an extremist nature, transnational organised crime, trafficking in human beings, illegal migration, international illicit trade in weapons, including weapons of mass destruction, ammunition and explosive materials, radioactive, nuclear, toxic, narcotic, psychotropic and precursors, other goods, technologies and services of strategic importance for the security of the Republic of Moldova and the maintenance of international peace and security, as well as the fight against crimes endangering the security and interests of the State;

7) carrying out other activities of national, international and international interest.

Article 47. The basis for external intelligence activity

The basis for carrying out external intelligence work should be:

1) information which has become known to the Service concerning activities outside the country or initiated from outside which constitutes or could constitute a threat to national security, being prepared, committed or committed, concerning persons preparing, committing or commissioning it, and the need to establish such information;

2) information known to the Service concerning the whereabouts of persons announced in national, inter-state or international search for terrorist offences, crimes against the peace and security of humanity, public authorities and state security, organised crime, trafficking in human beings, international illicit trade in weapons, radioactive, nuclear, toxic, narcotic, psychotropic and precursor substances, technologies and services of strategic importance, other crimes undermining national or international security, and the need to establish such information;

3) the detection of signs relating to the conduct of informative or subversive activities outside the country or initiated from outside by, or on behalf of, foreign States or special services, governmental or non-governmental organisations, as well as individuals or special groups, of other activities which constitute or could constitute a threat to national security, and the need to prevent and combat the existence of such signs;

4) the need to plan, collect, verify, process, analyse, evaluate, retain and valorise information relevant for the national security, foreign and internal policy of the State;

5) the need to identify, prevent and combat unauthorised access to state secret information;

6) the need to identify, prevent and combat attacks on the security of the Republic of Moldova's special communications networks and to ensure cryptographic and technical protection of information;

7) the need to identify, prevent and combat terrorism, actions against the sovereignty and integrity of the Republic of Moldova, other activities of an extremist nature, transnational organised crime, trafficking in human beings, international illicit trade in weapons, including weapons of mass destruction, ammunition and explosives, radioactive, nuclear, toxic, narcotic, psychotropic and precursors, in other goods, technologies and services of strategic importance for the security of the Republic of Moldova and for the maintenance of international peace and security, as well as crimes which threaten, from the outside, the security and interests of the State;

8) the need to identify, prevent and combat the disruption to the security of the functioning of the institutions of the Republic of Moldova abroad and their employees, members of their families, as well as citizens located outside the boundaries of the Republic who have or have had access to state-secret information.

Article 48. Measures to carry out external intelligence activity

(1) The service shall be authorised to create, procure, own and use specific means, methods and sources for the planning, collection, verification, processing, analysis, evaluation, retention and exploitation of the information data needed to carry out the external intelligence activity.

(2) In carrying out the external intelligence activity, the Service shall apply operational methods and measures, technical and informative measures and influence measures specific to the type of activity, as well as appropriate technical and operational means to ensure the planning, collection, verification, processing, analysis, evaluation, retention and exploitation of information data.

(3) In the context of external intelligence activities, counterintelligence measures may be carried out in accordance with the requirements laid down in this Law.

(4) Information systems, databases, video recorders, audio cameras, photographers and other modern methods and means necessary to carry out the tasks of the given activity may be used in carrying out the external intelligence activity.

(5) Intelligence officers shall participate personally in the organisation and implementation of measures to carry out the external intelligence activity, drawing, where appropriate, on the assistance of officials and specialists in different fields of knowledge, as well as persons who collaborate confidentially with the Service.

Article 49. The conditions and the way in which external intelligence activity is carried out

(1) Measures to carry out external intelligence activities shall be permitted only for the purpose of carrying out the tasks of this Law.

(2) The decision on the application of the measures and methods for carrying out the external intelligence activity shall be taken by the Director of the Service or the Special Deputy Director.

(3) Measures to carry out external intelligence activities in the event of danger to the life, health or property of intelligence officers, of the institutions of the Republic of Moldova abroad, of citizens located outside the boundaries of the Republic who have or have had access to state-secret information, persons providing support to the Service and members of their families shall be authorised in accordance with the procedure laid down in paragraph (2).

(4) The external intelligence activity is carried out from the territory of the Republic of Moldova and from abroad.

(5) In carrying out the external intelligence activity, specialised subdivisions of other public authorities may also be involved, in accordance with the law, exclusively under the direct direction of the Service.

Chapter IV
FINANCIAL, TECHNICAL, MATERIAL AND SCIENTIFIC RESOURCES OF INTELLIGENCE AND COUNTERINTELLIGENCE ACTIVITYY

Article 50. Financial and technical-material resources of intelligence/counterintelligence

(1) The financial and technical and material resources of the intelligence/counterintelligence activity shall be carried out by the financial means allocated to the State Budget Service, in accordance with the Law on the Intelligence and Security Service of the Republic of Moldova, and by the special means obtained in accordance with the law.

(2) Financial and technical and material resources for intelligence/counterintelligence activities shall be examined and approved in closed meetings of the competent authorities, shall constitute State secrecy and may not be made public.

(3) Control of the expenditure on the financial means allocated to ensuring the provision of intelligence/counterintelligence activities shall be carried out by the Director of the Service, including through the internal control subdivision, by the Court of Auditors at a closed hearing, in accordance with the Law on State secrecy, and shall in particular be based on the presence of supporting documents for the execution of expenditure. The monitoring carried out shall be carried out within the limits which do not permit disclosure of the methods of intelligence/counterintelligence or of persons collaborating confidentially with the Service, ongoing operations, operations that have been completed and knowledge of their implementation could affect the security of the State.

Article 51. Scientific assurance of intelligence/counterintelligence activity

(1) Technical and scientific findings or extra-judicial expertise may be carried out as part of the intelligence/counterintelligence activity.

(2) Technical and scientific findings are the work of a specialist carried out in order to explain facts or circumstances, to establish facts requiring the use of special knowledge in the context of intelligence/counterintelligence work.

(3) The specialist, when making the technical and scientific finding, does not resolve questions of a legal nature.

(4) The technical and scientific findings shall be drawn up and made in accordance with the provisions of this Law.

(5) Extra-judicial examinations shall be carried out and carried out in accordance with the legislation in force.

Article 52. Grounds for ordering and carrying out the technical and scientific finding

(1) The technical and scientific findings shall be ordered if, in order to determine the circumstances which may be relevant to the conduct of the intelligence/counterintelligence activity, special knowledge in a field of activity is required.

(2) The technical and scientific findings shall be made on the basis of the written instruction of the intelligence officer carrying out the intelligence/counterintelligence activity.

(3) The provision for the technical and scientific finding must state the circumstances, the circumstances of the facts and the questions to be answered by the specialist, together with the materials to be investigated.

Article 53. Authorised subjects with the right to make technical and scientific findings

(1) The technical and scientific findings are carried out by specialists from the Service.

(2) If there are no specialists within the Service with special knowledge in a particular field of activity, or if the complexity of the case so requires, the technical and scientific finding may be ordered from specialists outside the Service.

(3) Technical and scientific findings may be made to professionals outside the Service only if they agree to do so on the basis of an agreement or contract.

Article 54. Organisation and performance of technical and scientific findings

(1) Upon receipt of the provision to carry out the technical and scientific finding, the head of the technical and scientific finding subunit shall appoint a specialist who has the skills and knowledge necessary to carry out it.

(2) The specialist who has received the instruction to carry out the technical and scientific finding and the related materials shall record it and, within 3 days, shall present himself or herself with the skills and knowledge necessary to make the finding.

(3) If necessary, the specialist may request additional information and material from the authorising officer of the finding.

(4) When making the technical and scientific findings, the same rules, methodics and machines shall be used as when carrying out judicial expertise.

(5) After examining the material received and taking appropriate action, the expert shall draw up a report setting out the questions referred, explaining the facts, unclear circumstances, establishing the facts.

(6) The technical and scientific findings report shall contain information on:

a) the identification of the specialist;

b) data on the studies or qualifications held by the specialist to conduct research and experience in the field;

c) details of the authorising officer of the finding;

d) questions submitted for consideration;

e) the circumstances and circumstances of the factual situation;

f) research carried out with a description of the research methods applied;

g) conclusions.

(7) The results of the technical and scientific findings shall be used to achieve the purposes of the intelligence/counterintelligence activity.

Chapter V
SPECIAL DATA PROTECTION RULES OF A PERSONAL NATURE

Article 55. Control over the processing of personal data in the framework of the intelligence/counterintelligence activity

(1) Control over the processing of personal data in the context of intelligence/counterintelligence activities shall be carried out exclusively in accordance with the provisions of this Law.

(2) The processing of personal data in the context of the intelligence/counterintelligence activity is not subject to personal data protection legislation.

(3) Persons who have access or become aware of the personal data of the person who is the subject of the intelligence/counterintelligence activity are under an obligation to preserve the confidentiality of such data.

(4) The mechanism for recording and monitoring the processing of personal data in the context of intelligence/counterintelligence activities shall be established by means of a departmental legislative act.

Article 56. Protection of personal data not related to national security threats

(1) The service deletes personal data collected as part of the intelligence/counterintelligence activity as soon as it is found that they are not related to national security threats.

(2) Information on personal data, privacy, honour and reputation, known incidentally in the context of obtaining the data necessary for the performance of the tasks of the Service, if it is not relevant to the security of the State, may not be made public, stored or archived and the medium on which it is recorded will be destroyed or deleted, as the case may be.

Chapter VI
CONTROL OF INTELLIGENCE AND COUNTERINTELLIGENCE ACTIVITY

Article 57. Parliamentary control

(1) Parliamentary control of the intelligence/counterintelligence activity is exercised by the National Security, Defence and Public Order Committee, through the Subcommittee on Parliamentary Control over the work of the Intelligence and Security Service of the Republic of Moldova (hereafter – Parliamentary Subcommittee).

(2) The Director of the Service shall submit annually, at a closed sitting, a general report to the parliamentary subcommittee on the intelligence/counterintelligence activity, which shall include, on a compulsory basis, information on the total number of counterintelligence measures carried out, the number of counterintelligence measures, laid down in Article 12 (1), carried out by measure.

(3) The parliamentary subcommittee may ask the President of the Chisinau District Court and the Chisinau Court of Appeal for information on the number of counterintelligence measures for which a judicial warrant has been issued and the number refused to be authorised.

(4) Following the presentation of the report, members of the parliamentary subcommittee may submit questions about the intelligence/counterintelligence activity carried out by the Service in the previous year. Information on the completed operations carried out by the Service may be presented at the hearing if their disclosure will not prejudice the security of the State. Information on ongoing operations is not provided.

(5) On the basis of the report submitted, the parliamentary subcommittee may make recommendations on the work of the Service.

(6) The report submitted to the parliamentary subcommittee may be made public, excluding from it information attributed by the state secret.

Article 58. Control by the public prosecutor

(1) The public prosecutor’s control of the counterintelligence activity shall be carried out by prosecutors of the Prosecutor General’s Office, specifically empowered to do so by the Prosecutor General.

(2) The check shall be carried out on the basis of complaints lodged by persons whose rights and legitimate interests are presumed to have been infringed or of their own motion, where the public prosecutor has become aware of the infringement when carrying out counterintelligence measures, if such acts may constitute criminal offences.

(3) During the check, information on the activity of persons who have cooperated or collaborated confidentially with the Service may only be submitted to a prosecutor in the category referred to in paragraph (1), specifically authorised to do so by order of the

Prosecutor General. The information shall be provided only if it is directly related to the subject matter of the control carried out and only if it is absolutely necessary to carry out the control.

(4) The prosecutors, who pre-empt the power to exercise control over the counterintelligence activity, will improve the right of access to state secrecy, if they do not have such a right at the moment, and will be subject to verification in accordance with the provisions of Law No 271/2008 on the verification of holders and candidates for public office, irrespective of the date of the last check.

Article 59. Internal Control

(1) Internal control of the intelligence/counterintelligence activity shall be carried out by the Director of the Service, the Deputy Director specifically empowered, including through the internal control subdivisions and the heads of the specialised subdivisions.

(2) Persons not directly involved in working with persons who cooperate confidentially with the Service, including the Director and Deputy Directors of the Service, shall not have the right to request information about their actual identity unless it is dictated by an urgent need for the service.

Article 60. Control by judges

The review carried out by judges shall be carried out by checking whether the counterintelligence measures to issue the court warrant are well founded or when assessing the legality of actions carried out in the absence of a judicial warrant.

CHAPTER VII
FINAL AND TRANSITIONAL PROVISIONS

Article 61.

(1) This Law shall enter into force 30 days after its publication.

(2) Within 30 days of the date of publication of this Law, the Intelligence and Security Service of the Republic of Moldova, the Judecătoria Chisinau, the Court of Appeal of Chisinau and the General Prosecutor’s Office shall take the necessary measures pursuant to Articles 15 (3) and (15) and 58 (4).

(3) The Government shall, within 6 months of the date of publication of this Law, submit to Parliament proposals to bring the legislation into force in line with this Law.

The President of Parliament

Informative Note
on the draft of Law on Counterintelligence
and external intelligence activity

The Law on Counterintelligence and External Intelligence activity is the legislative initiative of the President of the Republic of Moldova drawn up with the support of the Intelligence and Security Service.

The conditions governing the preparation of the draft legislative act and the objectives pursued

The project aims to delimit the competences of the SIS and adjust them to the standards of special services of countries with enhanced democracy, and to adjust the intelligence and counterintelligence process to the dynamics of risks and threats affecting national security.

In accordance with Article 8 of Law No 753 of 23.12.1999 on the Intelligence and Security Service of the Republic of Moldova, in order to carry out tasks relating to the provision of State security, the SIS carries out intelligence and counterintelligence activities. The way in which intelligence and counterintelligence measures are carried out, as well as the conditions for the use of secret methods and means in the conduct of intelligence and counterintelligence activities will be determined by the legislation.

There is currently no separate piece of legislation regulating the conduct of counterintelligence and external intelligence activity, as the Service carries out the tasks laid down by the legislation through special investigative measures, pursuant to Act No 59 of 29.03.2012 on special investigative activity.

At the same time, such a practice is not welcome, as the special investigative activity has as its primary purpose the prevention and detection of crimes. Nevertheless, the tactics and the mechanism for ensuring public order, detecting criminal offences cannot be applied effectively in carrying out the tasks of ensuring State security. In this regard, the opinion of Mr Goran Klemencic, an expert of the Council of Europe, who in 2006 carried out an analysis of the Law on Operational Investigative Activity, points out that it *must be a legislative and institutional separation of the supervision carried out by the legal bodies for the purposes of criminal investigations and surveillance carried out by intelligence services for national security purposes*.

In the same context, the experts of the Venice Commission Iain CAMERON, Ian Leigh and Mikael LYNGBO, who carried out the expertise of the draft Law amending and supplementing certain legislative acts (Law No 753/1999 and Law No 59/2012) expressly mentioned: *The Venice Commission and the Directorate consider it legitimate that the Moldovan authorities wish to establish a new mechanism for security investigations with a view to lifting the Service's special investigative measures outside the criminal investigation framework*.

As the European Court of Human Rights has also reported, *"democratic societies are under threat, today by complex forms of espionage and terrorism, so the state must be able, in order to combat these threats effectively, to secretly oversee the subversive elements operating in its territory. The existence of legislative provisions granting powers of secret supervision of correspondence and communications is necessary in a democratic society in order to ensure national security*."

The Convention leaves the States a certain degree of discretion, as regards the detailed rules of the system of monitoring, merely requiring the existence of adequate and sufficient safeguards against abuse.

Regional and international practice shows eloquently the existence of a huge complex of risks and threats to a state and its population. The threats of international terrorism exist in all states, regardless of their geographical location and foreign policy.

In addition, it is impossible to deny the major danger emanating from non-state forces, which through various mechanisms incite extremist forces inside a state to act separatist extremist and erode its foundations.

Thus, the creation in the Republic of Moldova a viable and enhanced mechanism to prevent and counteract any threat to the security of the state and the citizen, from outside, and from within the country, is fully justified.

Main provisions of the project and outline of new elements

The draft law establishes the mechanism for carrying out counterintelligence and external intelligence activity, as well as to create an appropriate system of safeguards and control over the performance of these activities, in order to prevent any possible abuse. At the same time, the system, while providing control over counterintelligence and external intelligence activities, must not overly bureaucratize the work carried out or constitute an artificial obstacle to the operational performance of tasks carried out in the interests of State security.

The draft law is structured in 7 chapters, detailing in each chapter a specific segment of the intelligence and counterintelligence activity, ensuring its performance or control over compliance with the law when carrying out this activity.

The first chapter defines the concepts of counterintelligence and external intelligence activity, indicating that they are carried out solely for the purpose of gathering information necessary for the performance of State security tasks.

Exclusively SIS intelligence officers will carry out the activities concerned. It also includes rules governing the status and guarantees of persons who collaborate confidentially with the Service in carrying out tasks relating to the security of the State.

For the purpose of the efficient performance of the intelligence/counterintelligence activity, the project sets out the concrete obligations of postal service providers and providers of electronic communications networks and/or services, covering the assistance provided in its conduct. Those obligations are not new for the legal persons concerned and will not constitute an additional burden for them, since such obligations also existed, pursuant to Article 16 (2) of Law No nr.59/2012 on special investigative activity, Article 20 (3) of Law No 241-XVI of 15 November 2007 on the special activity of investigations, and Joint Order No 44, MIA and CCCEC No, 249, 91 of 14.07.2008 ‘To approve the instruction on how to organise and carry out operational investigative measures in electronic communications networks’.

The project provides for the establishment of a court warrant, a new institution of law, which is the authorisation of the court to carry out counterintelligence measures that seriously interfere in private life. The court warrant is to be issued, on the basis of a reasoned approach by the director of the Service, by a special judge empowered to do so.

Counterintelligence measures which may be carried out with a judicial warrant are expressly laid down in the law and are carried out when monitoring and investigating the place of residence or communications made by individuals through different communication systems – verbal, electronic, postal, etc.

Taking into account the remarks made by the ECtHR in the case of Iordachi and Others v. Moldova, as well as the proposals put forward by the Venice Commission experts, who have previously studied two projects with similar rules, it is expressly and clearly determined the categories of persons in respect of whom counterintelligence measures may be carried out. In this way, judicial mandates will be issued in respect of those persons who are aware of the planning or contempt of facts posing a particular danger to the security of the State and endangering public security.

Likewise, are regulated counterintelligence measures, which may be carried out with the authorisation of the Director of the Service or the Assistant Director. The authorisation in question will be issued by order at the substantiated approach of the intelligence officer.

The grounds for initiating the counterintelligence activity stem from the tasks of the Service established by legislative acts.

At the same time, a maximum time limit for which a certain measure may be authorised has been set. The implementation of all counterintelligence measures shall be recorded in a report, the constituent elements of which shall be laid down by law.

The draft enshrines the concept of the use of information acquired, as a result of counterintelligence measures, exclusively in the performance of activities relating to the provision of State security. That information cannot be presented as evidence in a criminal case. If the counterintelligence activity establishes the constituent elements of a criminal offence, the Service will refer the matter to the Public Prosecutor’s Office with a view to initiating the special investigation or, as the case may be, the criminal procedural measures.

An innovative element is the duty of the Service to inform the individual that a counterintelligence measure involving an interference with his or her private life has been

carried out. At the same time, if the information will endanger the security of the State, another investigation carried out or the purpose of the measure carried out, or will present a danger to the life of the person, it will not be done, however, the final decision will be left to the judge and not to the Service.

In order to avoid interpretation in the process of carrying out the counterintelligence work, all counterintelligence measures have been defined, setting out in detail the actions to be taken when carrying out one or other measure.

It should be noted that the project regulates for the first time such a segment of the activity of a special service, such as external intelligence activity. This type of activity is carried out outside the Republic of Moldova for the purpose of knowing the intentions of individual states and individuals vis-à-vis the Republic of Moldova.

The project expressly sets out the tasks of the external intelligence activity and the basis for its conduct. Measures to carry out external intelligence activities, as well as the conditions and the manner in which it is to be carried out, are also regulated.

A special place is provided for the regulation of the technical and scientific provision of intelligence and counterintelligence.

The draft law also regulates the mechanism for processing personal data in the context of the intelligence/counterintelligence activity. Due to the specific nature of the activity relating to the provision of State security, considering that personal data processed in the course of that activity are protected by the legal regime of State secrecy, the field of processing of personal data in the intelligence/counterintelligence activity is not subject to the general legal regime of protection and control over the processing of the data in question. This derogation from the general rule also corresponds to the practice of other States and international rulers.

In order to ensure that the measures taken in the context of the intelligence/counterintelligence activity do not degenerate into abuse of service, in addition to all the above mentioned conditions, the procedure for monitoring the activity concerned shall also be regulated. The main type of scrutiny is to be parliamentary scrutiny, which will be carried out by the Subcommittee for the exercise of parliamentary control over the work of the Intelligence and Security Service. In accordance with the proposed rules, the Director of the Service will report annually on the intelligence/counterintelligence work carried out by the Service.

Furthermore, in the case of complaints from citizens concerning abuses by the Service or in the case of self-reporting, specially appointed prosecutors from the General Prosecutors will be able to carry out checks on the legality of the actions of intelligence officers.

At the same time, there will be permanent internal control within the Service by the director of the Service and by special sub-units with monitoring, analysis and control functions.

As regards the financial control of intelligence/counterintelligence activities, this will be carried out through public internal financial control and by the Court of Auditors.

In preparing the project, best practices laid down in the legislation of other States, such as Romania, Ukraine, Lithuania, France, Slovakia, Croatia, Germany, Spain, Montenegro, Hungary, as well as in international acts such as Council of Europe Recommendation (2005) 10 on “Special Investigation Techniques”, ECtHR cases Klass and Others v. the Federal Republic of Germany, Leander v. Sweden, Kennedy v. the United Kingdom, Rotaru v. Romania, Amann v. Switzerland, Iordachi and Others v. the Republic of Moldova, Krislin v. France, Malone v. the United Kingdom, Huvig v. France, etc. have been taken on board.

An exchange of information on the issue was also carried out with colleagues from France, Romania, the United Kingdom, Poland and Germany.

At the same time, was taken into account the recommendations set out in the Joint Opinion of the Venice Commission, the Directorate for Information Society and Fight against Crime and the Directorate for Human Rights (HRDs) of the Council of Europe’s Directorate-General for Human Rights and Rule of Law, on draft Law No 281 amending and supplementing the Moldovan legislation on the so-called “Security Mandate” of March 2017.

In addition, the draft law will be sent to the Venice Commission experts for consultation.

Economic and financial rationale

Additional financial sources are not needed to implement the draft law.

The adoption of the draft Law on counterintelligence and external intelligence activity will improve the mechanism for the Intelligence and Security Service to fulfil its legal duties, leading to the strengthening of state security and the exclusion of possibilities for abuse by intelligence officers or other decision-makers.