Strasbourg, 7 September 2023 **CDL-REF(2023)034**

Engl. only

EUROPEAN COMMISSION FOR DEMOCRACY THROUGH LAW
(VENICE COMMISSION)

REPUBLIC OF MOLDOVA

The Law on Counterintelligence and External Intelligence Activity

CDL-REF(2023)034

L A W
on counterintelligence and external intelligence activity

The Parliament adopts this Organic Law.

Chapter I
GENERAL PROVISIONS

Article 1. Notions, purpose and regulatory scope

(1) This Law lays down the legal framework for the counterintelligence activity and external intelligence activity (hereinafter – *intelligence/counterintelligence activity*), carried out by the Security and Intelligence Service of the Republic of Moldova (hereinafter – *the Service*), or, where appropriate, by the Ministry of Defence, the way and conditions for ordering and carrying out counterintelligence measures and external intelligence measures, and checking the legality thereof, the minimum protection guarantees of individuals subject to counterintelligence measures.

(2) The counterintelligence activity shall consist of all the measures, actions, operations, and procedures carried out by the Service in order to identify, prevent and counteract the vulnerabilities, the risk factors and the threats, in compliance with the scope of Law no.136/2023 on the Security and Intelligence Service of the Republic of Moldova.

(3) External intelligence activity shall consist of all measures, actions and operations carried out for planning, collection, verification, evaluation, analytical processing, storage, keeping and exploitation of data and information about actual or potential possibilities, actions, plans or intentions of foreign states or organisations, unconstitutional entities or individuals that constitute or might constitute risk factors or threats to the security of the Republic of Moldova, as well as for obtaining the information relevant to the provision of national security or the creation of conditions conducive to ensuring and promoting strategic interests and the successful implementation of the Republic of Moldova's security policy.

(4) Carrying out intelligence/counterintelligence activity for purposes other than indicated in this Law shall not be allowed.

Article 2. Principles of carrying out intelligence/counterintelligence activity

The intelligence/counterintelligence activity shall be carried out according to the following principles:

a) legality;
b) equality before the law for all;
c) respect for human rights and freedoms and the regulation of the limitation of their exercise exclusively by law;
d) political neutrality and impartiality;
e) combination of methods and means of public and secret activity;
f) opportunity;
g) proportionality;
h) active nature of the measures carried out;
i) confidentiality;
j) efficiency and effectiveness.

Article 3. Subjects carrying out intelligence/counterintelligence activity

(1) The intelligence/counterintelligence activity shall be carried out by the Service through the intelligence and security officers (hereinafter – *intelligence officers*) of its specialised subunits.

(2) The external intelligence activity in the military field shall be carried out by the Ministry of Defence through contracted servicemen within its specialised bodies and structures.

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

Article 4. Rights, powers, and obligations of the subjects carrying out the intelligence/counterintelligence activity

(1) In carrying out the intelligence/counterintelligence activity, the Service and the intelligence officers shall have the rights, powers and obligations set out in Law no.136/2023 on the Security and Intelligence 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 external intelligence activity in the military field, the Ministry of Defence and the contracted servicemen shall have the rights, powers and obligations set out in Law no.162/2005 on the status of servicemen and in other normative acts in the defence field.

Article 5. Use of technical means for carrying out the intelligence/counterintelligence activity

In carrying out the intelligence/counterintelligence activity, the use of information systems, special technical means for covert obtaining of information, video/audio recording devices and other technical means shall be permitted.

Article 6. Special file

(1) In order to collect and systematise the information, to check and assess the results of the intelligence/counterintelligence activity and take the appropriate decisions on the basis thereof, special files shall be initiated with all the collected information and materials attached thereto. The opening of the special file shall be subject to compulsory registration.

(2) The special file shall be initiated on the basis of:

a) the report of the intelligence officer from the specialised subunit, approved by the Director of the Service or the empowered Deputy Director;

b) the report of the contracted serviceman from the specialised bodies and structures of the Ministry of Defence, approved by the head of the respective body or structure.

The special file shall be deemed initiated as of the date of its registration.

(3) The counterintelligence measures and the external intelligence measures cannot be carried out outside a special file.

(4) Each special file shall entail a mechanism for record-keeping of individuals who have become acquainted with the file information and materials, which shall include at least:

a) name, surname and position of the respective individual;
b) date and time of starting to study the information and materials of the file and date and time of its completion;
c) notes relating to the access to the entire special file, certain documents, or compartments thereof,
d) signature of the respective individual.

(5) The Service and the Ministry of Defence shall ensure the necessary measures to protect the information and materials held in the special files against disclosure, modification, or unauthorised destruction.

Article 7. Management of the classified special file

(1) After the classification, the special file shall be retained in the special storage of the Service or, where appropriate, the storage of the Ministry of Defence. The storage term of the classified special file shall be equal to the secrecy period.

(2) After the expiration of the storage term of the classified special file, the decision on the extension of the secrecy period shall be taken, pursuant to Law no.245/2008 on the state secrecy, or on the destruction thereof. If the information and materials of the file have historic or scientific value, these shall be declassified and transferred for safekeeping to the National Archive of the Republic of Moldova.

Article 8. Departmental regulation of intelligence/counterintelligence activity

The organisation, methods for carrying out counterintelligence and external intelligence measures; internal authorisation procedures, rules for drawing up minutes on the management, retention and destruction of information and materials obtained, measures for ensuring the integrity and confidentiality thereof, and of intelligence/counterintelligence activities; rules for carrying out covert operations and on the conduct and management of covert activities; the way of registering special files, their category, initiation, management, classifying, the time limits for their retention and the procedure for their destruction; the use of financial resources assigned for carrying out counterintelligence and external intelligence measures; the method of working with individuals collaborating confidentially with the Service, or, where appropriate, the Ministry of Defence, including the way in which the information submitted by them is documented, the categories of such individuals; the organisation, the staff, resources, sources, plans, procedures, tactics, methods and means of carrying out the intelligence/counterintelligence activity, as well as the use of the results thereof, shall represent information assigned to the state secrecy and shall be regulated by the internal acts of the Service, or, where appropriate, the Ministry of Defence.

Chapter II
COUNTERINTELLIGENCE MEASURES

Section I
Authorisation of counterintelligence measures

Article 9. Counterintelligence measures

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

1) by the authorisation of the Director of the Service or the empowered Deputy Director – identification of the subscriber or the user of an electronic communications network or of an information society's service;

2) by court warrant:

a) scrutiny of the domicile and/or, where appropriate, the installation therein of devices for video/audio surveillance, photography, or the ascertainment of factual circumstances;

b) domicile surveillance by using technical means;

c) interception of communications;

d) access to information held or processed within an information system, on communication devices or equipment, and/or its monitoring;

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

f) the retention, investigation, handover, search, or withdrawal of postal items;

g) video/audio recording of the content of communications;

h) blocking the access to electronic communications networks for an information system, device or equipment, or for an information society, blocking of electronic communications services;

i) operative withdrawal;

j) obtaining the access to financial information or monitoring financial transactions;

k) visual tracking and/or documentation by technical methods and means, as well as positions or tracking through the global positioning system or other technical means.

(2) The list of measures listed in para (1) is exhaustive and shall be amended or supplemented by law only.

Article 10. Grounds for carrying out counterintelligence measures

The grounds for carrying out counterintelligence measures include:

1) the information concerning:

a) the risks under Article 4 para (2) of the Law on the state security no.618/1995 and the deeds listed under Article 3 p.2), letters b) and c) of Law no.136/2023 on the Security and Intelligence Service of the Republic of Moldova;

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

2) interpellations of international organisations or legal authorities of other States, in accordance with the 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;

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

4) protection of state secrecy;

5) collection of the necessary information on the individuals subject to verification with respect to:

a) granting access to information falling under state secrecy;

b) admission to work at critical infrastructure facilities;

c) establishing or maintaining collaboration relationships in the organisation and conducting counterintelligence and/or external intelligence measures;

6) screening of candidates or holders of public office;

7) ensuring internal security;

8) collecting the necessary information on the individuals collaborating confidentially with the Service, as well as on the individuals subject to verification for the admission to the organisation and conduct of certain counterintelligence and/or external intelligence measures, or for granting access to the information and materials collected in the course of these measures' implementation.

Article 11. Procedure for the authorisation of counterintelligence measures by the Director of the Service or the empowered Deputy Director

(1) The conduct of the counterintelligence measure referred to in Article 9 para (1) subpara (1) shall be authorised, by order, by the Director of the Service or the empowered Deputy Director, based on the approach of the head of the subunit carrying out the counterintelligence activity under an opened and registered special file.

(2) The approach indicated under para (1) shall include: factual circumstances serving as grounds for carrying out counterintelligence measures; the reasoning for the need of the respective measure; the number of the special file under which the counterintelligence measure is to be carried out.

(3) For the issuance of the order indicated under para (1), the Director of the Service or the empowered Deputy Director, shall additionally consider, besides the validity of the approach, whether:

a) the requested measure pursues a legitimate purpose;

b) the measure is proportional to the restriction of the exercise of the individual's rights or freedoms guaranteed by law, and to the need of its performance.

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

a) the date of issue;

b) the number of the special file under which the counterintelligence measure is authorised;

c) the authorised counterintelligence measure.

(5) The Director of the Service, the empowered Deputy Director shall deny the authorisation of the counterintelligence measure if they find that the submitted approach is groundless, does not pursue a legitimate purpose or the requested measure is disproportionate in relation to the restriction of the exercise of the individual's rights or freedoms.

Article 12. Procedure for authorising counterintelligence measures by issuing a court warrant

(1) For the purpose of this Law, the court warrant represents the authorisation to carry out, under a special file opened and registered, the counterintelligence measures provided under Article 9 para (1), subpara 2).

(2) The court warrant shall be issued, based on a written approach of the Director of the Service or the empowered Deputy Director, by a judge of the Chisinau Court of Appeal appointed for this purpose.

(3) The approach for issuing the court warrant shall contain the following data:

(a) name, surname and position of the individual applying for the issue of the court warrant;

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

c) the status of lawyer or journalist held by the individual subject to the counterintelligence measure and the factual circumstances excluding the incidence of the prohibition under para (6);

d) the counterintelligence measure for which authorisation is requested;

e) the factual circumstances serving as the basis for carrying out the counterintelligence measure and, where appropriate, the possible consequences thereof;

f) the argumentation of the proportionality of the counterintelligence measure for which the authorisation is requested, with the restriction of the individual's exercise of rights and freedoms;

g) in the case of a request for an extension of the term for carrying out the counterintelligence measure, the grounds and reasons justifying the extension;

h) the expected outcomes following the conduct of the counterintelligence measure;

i) the period of carrying out the respective measure;

j) the place of the counterintelligence measure carrying out;

k) other information relevant to justify the counterintelligence measure and support the legality and the grounds for its authorisation.

(4) The examination of the approach for the court warrant issue shall be performed within 24 hours. At the request of the judge, the intelligence officer also participates in the examination of the approach, presenting the necessary explanations. During the examination of the approach, the judge shall be submitted, upon own request or at the initiative of the Service, the information and materials justifying the need to carry out the respective measure, without revealing the identification data of individuals who collaborate confidentially with the Service.

(5) In order to issue the court warrant, the judge shall further verify whether:

a) the requested action pursues a legitimate purpose;

b) the achievement of the purpose provided for by this law is impossible in any other way;

c) the requested measure is proportional to the restriction of the exercise of fundamental rights and freedoms.

(6) The authorisation of the conduct of counterintelligence measures shall be prohibited:

a) with regard to the legal relations of legal assistance between lawyers and their clients;

b) with regard to journalists, with the purpose of establishing their sources of information.

(7) The information falling under para (6), which were accidentally collected, shall not be used by the Service, and shall be destroyed, under the authorisation of the judge.

(8) After verifying the legality and validity of the approach under para (2), the judge shall authorise, by ruling, the execution of the counterintelligence measure or reject the approach. Pursuant to the ruling on the authorisation, the judge shall issue a court warrant that is binding for execution.

(9) The court warrant shall be transmitted not later than 24 hours after the submission of the approach for its issuance. The reasoned ruling shall be drawn up and issued within 48 hours at most.

(10) The ruling under para (8) shall contain the following data: the date and place of the ruling drawing up; name and surname of the judge; name, surname and position of the individual applying for the issue of the warrant; the body entitled to carry out the counterintelligence measures; the identification data of the individual subject to counterintelligence measures, if known; the grounds and the reasons justifying the need to carry out and authorise the counterintelligence measures, respectively; the authorised counterintelligence measures; the period for carrying out the counterintelligence measures; the place of carrying out the counterintelligence measures; other data relevant for justifying the authorisation of counterintelligence measures.

(11) Counterintelligence measures, which may be carried out only based on a court warrant, may, by way of exception, be carried out, without the court warrant, based on a reasoned order of the Director of the Service or the empowered Deputy Director, in case of exceptional circumstances not allowing for its delay, and if the court warrant cannot be obtained without exposing to a substantial risk of delay which may lead to the loss of relevant information or imminently jeopardise the security of the State or of individuals. In such a case, the judge shall be informed within 24 hours from the

ordering of the counterintelligence about its performance, while being provided with all the information and materials substantiating the need to carry out the respective measure and the exceptional circumstances which have not allowed for its delay. Provided that there are sufficient grounds, the judge shall confirm, by means of a reasoned ruling, the legality of the counterintelligence measure performance. Otherwise, the judge shall declare the illegality of the respective measure performance.

(12) Counterintelligence measures initiated pursuant to para (11) shall be carried out until the judge's ruling is issued, while afterwards the proceedings shall be in accordance with the respective ruling.

(13) Simultaneously with the confirmation of the legality of the counterintelligence measures performance, the judge shall, at the request of the Director of the Service or the empowered Deputy Director, issue a court warrant on the authorisation of their further performance.

(14) When declaring the counterintelligence measures performance to be illegal, the implementation of the respective measure shall be stopped.

(15) The reasoned ruling of the judge on the rejection of the approach for the issue of the court warrant, as well as the reasoned ruling on declaring the illegality of the counterintelligence measure performance may be appealed by the Service to the Supreme Court of Justice.

(16) The appeal under para (15) shall be examined by a panel of three judges in accordance with para (4).

(17) The appeal under para (15) shall be lodged within three working days from the date of the reasoned ruling issue and shall contain the factual and legal grounds regarding the unsubstantiality and/or the illegality of the appealed ruling.

(18) After the examination of the appeal under para (15), the panel of the Supreme Court of Justice shall, by decision:

a) admit the appeal, quash the ruling and, where appropriate, issue a court warrant or declare the counterintelligence measures performance to be legal;

b) dismiss the appeal and uphold the ruling;

(19) The decision under para (18) shall be drawn up and issued in compliance with the provisions of para (9).

Article 13. Special conditions for carrying out counterintelligence measures authorised through the court warrant

(1) The carrying out of counterintelligence measures shall be authorised under the provisions of Article 10.

(2) Article 10 paras.4)–6) shall authorise the implementation of counterintelligence measures referred solely to in Article 9 para (1) subparas (1) and (2), letters e) and j).

(3) At the express consent or prior request, in written form, of the individuals who contribute to the conduct of intelligence/counterintelligence activity, the counterintelligence measures provided for by this Law can be carried out, both in relation to them and their relatives and family members, if there is an imminent risk to their life, health or other fundamental rights, or if the implementation of the respective measures is necessary to prevent a crime or adverse consequences in relation to those individuals.

Article 14. The period for which the conduct of counterintelligence measures is authorised

(1) The counterintelligence measures referred to in Article 9 para (1) subpara (2), which do not constitute one-off measures, with the exception of those referred to in Article 9 para (1) subpara 2) letter a), shall be authorised for a period of up to 90 days, with the possibility of its extension for successive periods and for non-successive periods of up to 90 days.

(2) The counterintelligence measure, as referred to in Article 9 para (1) subpara (2) letter a), shall be authorised for a period of up to 30 days, with the possibility of its extension for successive periods and for non-successive periods of up to 30 days.

(3) The total duration of the implementation of a counterintelligence measure with respect to an individual ordered on a concrete deed shall not exceed 24 months cumulatively, while its completion cannot take place later than 4 years from the initiation of the measure. During each

request for the extension of the period for carrying out the counterintelligence measure, the judge shall be required to examine the grounds and the reasons justifying such an extension and, in case the request is deemed ungrounded, the judge shall reject the extension of the period.

(4) The carrying out of counterintelligence measures must begin on the date indicated in the act ordering them, or on the date of expiry of the period for which they have been authorised, at the latest.

Article 15. Termination of the counterintelligence measure performance before the deadline

The Director of the Service or the empowered Deputy Director shall command, through order, the termination of the counterintelligence measure before the expiry of the period for which a court warrant has been issued as soon as the grounds and reasons justifying the authorisation of the measure have disappeared. The termination before the deadline and the grounds for the early termination of the counterintelligence measure shall be brought to the knowledge of the judge who has issued the court warrant.

Article 16. Record of counterintelligence measures

(1) Following the completion of the counterintelligence measure implementation and establishing the lack of the need to further carry it out, or its termination before the deadline, the intelligence officer carrying out the counterintelligence measures shall draw up minutes for each authorised measure, recording the following:

a) the title of the counterintelligence measure carried out, the place and date on which it has been carried out, where appropriate, the time of its commencement and completion, details on the authorisation of the measure or the court warrant;

b) position, name, and surname of the intelligence officer drawing up the minutes. If the counterintelligence measure has been carried out directly by the intelligence officers of the subunits of intelligence/counterintelligence activity, who are part of the Service's cryptic staff, the minutes shall indicate the position, name, and surname of the head of the respective subunit, who verifies the correctness of the information mentioned in the minutes and signs it. The mentioned subunits shall keep strict records of the intelligence officers who have carried out counterintelligence measures and drawn up minutes;

c) the names, surnames and the status of individuals that participated in the carrying out of the measures. The respective data shall not be recorded in the minutes in relation to the intelligence officers from the subunits of intelligence/counterintelligence activity that are part of the Service's cryptic staff, nor in the cases of individuals confidentially collaborating with the Service;

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

e) the information on the use of technical means, the conditions and procedures for their application, the facilities where those means have been applied, the outcomes; and the note on the recording of the collected information.

(2) If the results of the counterintelligence measures are recorded, the information storage medium shall be attached to the minutes.

(3) The minutes and the information storage medium shall be attached to the special file.

Article 17. Verification of the legality of the implementation of counterintelligence measures by the judge

(1) After completing the implementation of the counterintelligence measure and establishing the lack of the need for its further performance, or after its termination before the deadline, the intelligence officer shall, in order to verify compliance with the legality of the measure, transmit, within 10 working days, to the judge who authorised the respective measure, the minutes on the counterintelligence measure, with the information and materials collected following its implementation attached thereto.

(2) In the process of the verification of the legality compliance, the judge shall establish whether the counterintelligence measure has been carried out: with respect to individuals and for the investigation of facts indicated in the approach for the court warrant issue; in compliance with the issued court warrant; in compliance with deadlines.

(3) If the measure was carried out in compliance with the legislation, the judge shall confirm, by ruling, the legality of the counterintelligence measure.

(4) If the judge establishes that the counterintelligence measure was carried out with the obvious violation of rights and freedoms of the individual or the provisions of the court warrant were transgressed, then, the judge shall declare, by ruling, the outcomes of the counterintelligence measure to be null, and notify the General Prosecutor's Office to investigate the admitted violations.

(5) The ruling on the declaration about the nullity of the outcomes of the counterintelligence measures can be appealed pursuant to the provisions of Article 12.

(6) The original version of the information storage medium containing the records of the data obtained, after the verification of legality according to this Article, shall be sealed by the judge and kept within the Service in a way that ensures the non-repudiation of the information and excludes the access of the intelligence officer who conducted the investigation of the case. A copy of the respective storage medium shall be attached to the special file. The original version of the information storage medium shall be presented during the control or can be used for other purposes, under the judge's authorisation, at the reasoned request of the Director of the Service or the empowered Deputy Director.

Article 18. Using the outcomes of counterintelligence measures

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

a) in carrying out the tasks of the Service;

b) in carrying out other counterintelligence measures.

(2) If, following the implementation of counterintelligence measures, a reasonable suspicion regarding the commission of a crime or the preparation of a crime commission is found, the prosecutor from the General Prosecutor's Office appointed for this purpose shall be immediately notified thereon through a report.

(3) The outcomes of counterintelligence measures under a special file may be used in another special file only with the authorisation of the judge who has issued the court warrant.

(4) The outcomes of counterintelligence measures shall not constitute evidence for criminal proceedings.

Article 19. Confidentiality of data on counterintelligence measures and external intelligence measures

(1) The information on the carrying out of counterintelligence measures and external intelligence measures, regarding the staff, resources, sources, means, methods, plans and outcomes of the intelligence/counterintelligence activity, as well as regarding the organisation, procedures, and tactics of carrying out counterintelligence measures and external intelligence measures, shall constitute state secrecy and may be declassified only in compliance with the legislation.

(2) Persons who are aware, by virtue of their position, status, circumstances, or by accident, of the performance of counterintelligence measures or external intelligence measures, or the outcomes thereof, must keep the confidentiality of the respective information.

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

Article 20. Notification of individuals about the counterintelligence measures taken against them

(1) Following the completion of the investigation of the case and the classification of the special file**,** and in the event of the performance of counterintelligence measures referred to in Article 9 para (1) subpara (2), the Service shall, within 5 working days from the date of the respective file classification, notify the individuals concerned. The materials confirming the notification of the individual shall be attached to the special file.

(2) The Service shall notify the judge who issued the court warrant about each case of individuals' notification according to para (1).

(3) The individual shall not be notified if there are reasonable grounds to believe that this could pose an essential risk to human life or health, jeopardise another ongoing investigation, harm the security of the State or prejudice the purpose for which the counterintelligence measures have been performed.

(4) The intelligence officer, who carried out the investigation of the case, shall draw up a written report on the existence of the grounds referred to in para (3), 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 request the judge who issued the court warrant to authorise the non-notification of the individual.

(5) After the examination of the approach made by the Director of the Service under para (4), the judge shall establish the presence or the lack of grounds for not notifying the individual, determine whether those grounds are permanent or provisional, and, where appropriate, authorise the non-notification of the individual or reject the approach. Depending on the permanent or provisional character of the established grounds, the judge may authorise permanent non-notification or non-notification for a determined period of time, but no longer than 1 year. Upon the expiry of the respective period, the Service shall be required to reassess the grounds for the individual's non-notification and take the necessary action, in accordance with the provisions of this Article, including, where appropriate, request the non-notification of the individual for a new period of time. The Service may appeal the rejection to authorise the individual's non-notification in compliance with the provisions of Article 12.

(6) If the grounds for not notifying the individual subject to the counterintelligence measure have disappeared prior to the expiry of the established period, the intelligence officer shall draw up a report and submit it for approval to the Director of the Service requesting the immediate notification of the individual in respect of whom the counterintelligence measure was carried out. If the report is approved, the individual shall be notified in accordance with para (1).

(7) The ruling of the judge authorising the individual's non-notification, as well as the reports approved by the Director of the Service shall be attached to the special file.

Section II
Counterintelligence measures

Article 21. Identification of the subscriber or user of an electronic communications network or of an information society's service

(1) The identification of the subscriber or user of an electronic communications network or of an information society's service shall consist of establishing the identification data of the subscriber, or user of an electronic communications network (International mobile subscriber identity (IMSI), the mobile phone number, the serial number of the subscriber identification module (the SIM card), the Internet Protocol (IP) address, physical addresses for the provision of the landline service), or of an information society's service, as well as the subscriber identification data (name, surname, IDNP, address), or in establishing whether an electronic communications service is active or was active on a certain date, or in establishing, without the electronic service provider's support, the presence of electronic communication means at an individual at a given time.

(2) If the counterintelligence measure is carried out with the support of an electronic service provider, they are submitted the extract from the corresponding order of the Director of the Service or the empowered Deputy Director regarding the authorisation of the measure, in which the type of information to be submitted is indicated. After receiving the extract from the order, the electronic service provider submits the requested information in the shortest possible time, without keeping a copy (including in electronic format) of the reply and submitted data.

Article 22. Scrutiny of the domicile and/or, where appropriate, the installation therein of devices for video/audio surveillance, photography, or the ascertainment of factual circumstances

(1) The scrutiny of the domicile and/or, where appropriate, the installation therein of devices for video/audio surveillance, photography, or the ascertainment of factual circumstances shall involve secret or undercover access to the domicile, without notifying the owner, the possessor or the individual living or staying in the respective domicile, for the purpose of installing the surveillance devices, as well inspecting the domicile to discover traces of activity, persons of interest in order to obtain other information necessary to establish the factual circumstances, observe and record events occurring in the domicile. The surveillance devices carry out the interception and the remote recording of the information, or the recording within the domicile, with subsequent removal thereof.

(2) In the context of the scrutiny of the domicile, samples for comparative research may be collected provided that this does not lead to the disclosure of the counterintelligence measure carried out.

(3) After the expiry of the period for the measure implementation, or in the event of measure termination before the deadline, secret or undercover domicile access shall be permitted, with prior authorisation from the Director of the Service, or the empowered Deputy Director, for the removal of the respective devices. In this case, the domicile shall not be scrutinised and no action other than the removal of the device shall be taken. A report shall be drawn up with respect to the entry into the home and the removal of devices, indicating the date and the individuals involved. The report shall be sent for information to the judge who authorised the respective measure.

(4) The removal of devices shall take place in the shortest time possible, after the expiry of the period for measure implementation or the termination of the measure. It shall be prohibited to use, in any way, the information recorded after the expiry of the period of measure implementation, or the termination of the measure, including viewing or hearing it, the information being immediately destroyed.

Article 23. Domicile surveillance by using technical means

The surveillance of the domicile by using technical means shall entail the supervision of the domicile from the outside, without the consent of the owner, the possessor or the individual residing or staying in the domicile, by using technical means, for the purpose of determining the events occurring in that home, conversations, other sounds or factual circumstances, recording the established facts.

Article 24. Interception of communications

(1) Interception of communications represents real-time access and monitoring of the content of communications made through the electronic communications networks or other technical means of communication, by recording the respective communications, as well as collecting, real-time recording of the type of communication, of traffic data and positioning data associated to the respective communications.

(2) The court warrant for the authorisation of the interception of communications shall additionally contain technical identifiers or identification data of the subscriber or the device used to intercept the communications.

Article 25. Carrying out and certifying the interception of communications

(1) The specialised subunit of the Service shall ensure the technical interception of communications, using software or special technical means connected, where necessary, to the equipment of the providers of electronic communications networks and/or services and/or of the intercepted individual. The intelligence officers of the subunit, who are in charge of the technical interception of communications, the employees directly listening to the records, viewing the information communicated, translating it, drawing up the verbatim report, shall keep the secrecy of the obtained information 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 in real time by the intelligence officer.

(3) The transcript represents the reproduction in writing of intercepted communications which are of importance for the special file. The transcript of communications shall contain the date, time and duration of the communication, names of the individuals whose communications are transcribed, if known, and other relevant data. The transcript shall be drawn up by the employees of the subunit of intelligence/counterintelligence activity and, if necessary or at the request of the intelligence officer carrying out the counterintelligence measure, personally by the latter.

(4) The intercepted communications shall be transcribed, as a rule, in the language in which the communication took place. If the communication has taken place in a language other than the Romanian language, the communication shall be translated into Romanian by a translator.

(5) The intelligence/counterintelligence activity subunit shall keep a strict record of the intelligence officers who have had access to the intercepted communication, and employees who have drawn up the transcript or translated the communication.

(6) Intercepted communications shall be fully retained on the initial medium presented by the specialised subunit to the intelligence officer. This medium shall be kept in the special file. The access to that medium shall be subject to record, comprising:

a) the name, surname, and position of individuals who have had access;

b) the date, and time of the initiation of access and the date, and time of termination of access;

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

d) the grounds/reasons for listening/viewing the information;

e) signature of individuals who have had access.

Article 26. Access to information located or processed within an information system, on communication devices or equipment, and/or its monitoring

(1) Access to the information on an information system, on communications devices or equipment shall require measures to be taken to allow obtaining the information from the information system, communications devices or equipment, or stored on another technical medium, by recording the necessary information on a tangible medium.

(2) The monitoring of information contained or processed in an information system, on communications devices or equipment, shall require measures to be taken to allow for the real-time monitoring of the actions undertaken within an information system, on the device or equipment, allow for the obtaining of the information under processing, as well as the information data associated with the respective actions.

(3) Access to the information found or processed within an information system, on communications devices or equipment and/or monitoring thereof may be carried out:

a) by establishing a permanent or temporary physical link between the specialised subunit of the Service and the equipment of the natural/legal person owning the information system, the communications devices or equipment, or the respective technical medium;

b) through software programmes;

c) by submitting directly to the holder of the information system, communications devices or equipment, or the technical medium, the extract of the court warrant issued by the judge concomitantly with the court warrant, indicating the type of information to be submitted.

(4) Access to the information located or processed in an information system or monitoring thereof cannot be achieved according to the provisions of this Article if this Law provides for another way of obtaining the respective information.

Article 27. 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 the assistance of providers of electronic communications services, the available information, generated or processed within the provision of own electronic

communications services , including roaming, necessary for the identification and tracking of the source of electronic communications for the 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:

a) telephone numbers registered in the name of an individual;
b) electronic communications services provided to the user;
c) electronic communication source (phone number or IP address of the caller);
d) the destination of the electronic communication (phone number or IP address of the caller; phone number to which the call is directed);
e) the type, date, time, and duration of the electronic communication, including failed call attempts. Failed call attempt shall mean the communication in which the call was successfully connected but not answered or an intervention related to the network management took place;
f) the user's electronic communications equipment or other device used for communication purposes (the IMEI codes of the caller's and the called individual's mobile phones; media access control address (MAC address) of the equipment of access to landline services at customer's premises (CPE); in the case of anonymous pre-pay services – the date and time when the service was initially activated and the name of the premises (Cell ID) from which the service was activated);
g) position of the mobile communication equipment (the premises name (Cell ID) from the beginning of the communication; the geographical position of the cell by reference to the name of the premises, during the period of data retention).

(2) The collection of information from providers of electronic communications services shall be carried out by presenting directly to the providers of electronic communications services the extract from the court warrant, issued by the judge concomitantly with the court warrant, indicating only the type of information to be submitted.

Article 28. Retention, investigation, handover, search or withdrawal of postal items

(1) The retention, investigation, handover, search, or withdrawal of postal items shall consist in 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 specified period, or delivering the postal item on a given date or time;

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

(2) During the implementation of the measures provided for in this article, the following shall be allowed:

a) performing the technical and scientific assessment enabling the identification of the objects or substances in the postal item, or other factual circumstances;

b) copying, recording on tangible medium, by using technical means, the information contained in the postal item;

c) sampling.

(3) The court warrant concerning the retention, investigation, delivery, search or withdrawal of postal items shall contain the name of the postal institution which is required to retain the postal items, the name and surname of the individual or individuals whose postal items are to be retained, the exact address of such individuals, if known, or other features on the basis of which the postal items, the type of postal items against which the counterintelligence measure is ordered, may be identified.

(4) Simultaneously with the court warrant, the judge shall also issue an extract thereof, which is sent to the head of the post office or postal delivery provider, for which the 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 intelligence officer about the retention of the postal items indicated in the extract of the court warrant, being required to ensure, and keep the confidentiality of the counterintelligence measure carried out.

Article 29. Video/audio recording of the content of communications

Video/audio recording of the content of communications shall entail the secret video/audio recording of communications transmitted by individuals in open spaces, in public places or in rooms, other than domicile, as well as communications transmitted to or in the presence of an intelligence officer, or an individual who collaborates confidentially with the Service, without having knowledge of their status.

Article 30. Blocking the access to electronic communications networks for an information system, device, or equipment, or for an information society, blocking of electronic communications services

(1) The blocking of the access to the electronic communications networks for an information system, a device, or an equipment, or for an information society, blocking of electronic communications services shall mean:

a) blocking the possibility of accessing some electronic communication networks by an information system, a device, or an equipment or by an information society;
b) suspension of an electronic communications service or an information society service for a telephone number, for a static Internet Protocol (IP) address, for an individual or physical address.

(2) The actions provided for in para (1) letter a) shall be carried out by the Service by using software or special technical means, and the actions provided for in para (1) letter b) shall be carried by the providers of electronic communications services, upon the presentation of the extract from the respective court warrant.

Article 31. Operative withdrawal

Operative withdrawal shall mean the secret withdrawal, with subsequent secret return, of goods, documents, and information tangible media for examination and analysis thereof, for technical and scientific assessment, collection of the necessary information and sampling and analysis of samples.

Article 32. Access to financial information or monitoring of financial transactions

(1) Access to financial information shall entail obtaining from banks, other individuals/organisations mediating financial transactions or other competent institutions, of documents or information in their possession relating to deposits, accounts, or transactions of an individual, or the movement of certain financial means.

(2) Monitoring of financial transactions shall represent the operations ensuring the knowledge, including real-time knowledge, of the content of financial transactions carried out through banks, other individuals/organisations mediating financial transactions, or other competent institutions with respect to deposits, accounts, or transactions of an individual, or the movement of certain financial means.

(3) Banks, other individuals/organisations meditating financial transactions, or other competent institutions shall be submitted the extract of the respective court warrant, indicating only the type of information to be submitted and, where appropriate, the period for carrying out the monitoring.

Article 33. Visual tracking and/or documentation by technical methods and means, as well as positioning or tracking through the global positioning system or other technical means

(1) Visual tracking and/or documentation using technical methods and means shall consist of the observation, by recording the observations, of buildings, facilities, means of transport, goods, actions/inactions of the individual, other factual circumstances taking place, with or without the use of technical recording means.

(2) Positioning of tracking through the global positioning system or other technical means shall consist of the use of technical devices to determine the position of the individual or object, as well as the monitoring of their movement or position, by recording of the acquired information.

CHAPTER III
EXTERNAL INTELLIGENCE ACTIVITY

Article 34. Tasks of external intelligence activity

The external intelligence activity shall have the task of detecting, preventing and counteracting external or external origin risk factors and threats to national security, and their consequences should they materialise, as well as protecting and promoting the strategic interests of the Republic of Moldova and its partners.

Article 35. External intelligence measures

The Service and the Ministry of Defence shall be entitled to create, procure, own and use specific tactics, methods, means and sources for the planning, collection, verification, evaluation, analytical processing, storage and exploitation of the information data necessary to carry out the external intelligence activity.

Article 36. The conditions and the way of carrying out the external intelligence activity

(1) Measures to carry out external intelligence activity shall be allowed only for the purpose of performing the tasks provided for in this Law.

(2) The performance of external intelligence measures and the enforcement of specific tactics, methods and means of performing the external intelligence activity shall be carried out in compliance with the internal acts of the Service, or, where appropriate, of the Ministry of Defence.

Chapter IV
FINANCIAL, TECHNICAL, MATERIAL AND SCIENTIFIC COVERAGE OF INTELLIGENCE /COUNTERINTELLIGENCE ACTIVITY

Article 37. Financial, technical and material coverage of intelligence/counterintelligence activity

(1) The financial, technical and material coverage of the intelligence/counterintelligence activity shall be carried out from the account of the financial means allocated to the Service, or, where appropriate, the Ministry of Defence, from the State Budget, in accordance with the legislation.

(2) The draft acts on financial, technical and material coverage of the intelligence/counterintelligence activity shall be examined and approved by the competent authorities in closed meetings, shall constitute state secrecy and may not be made public.

Article 38. Scientific coverage of intelligence/counterintelligence activity

(1) Technical and scientific assessment or extrajudicial expertise may be carried out within the performance of the intelligence/counterintelligence activity.

(2) Technical and scientific assessment within the intelligence/counterintelligence activity shall represent the work carried out by a specialist in order to explain facts or circumstances, observe certain situations involving special skills and knowledge.

(3) The specialist shall not solve matters of a legal nature while carrying out the technical and scientific assessment.

(4) The technical and scientific assessment shall be ordered and carried out in accordance with the provisions of this Law.

(5) Extrajudicial examinations shall be ordered and carried out in accordance with the legislation.

Article 39. Grounds for ordering and performing the technical and scientific assessment

(1) The technical and scientific assessment shall be performed pursuant to the written instruction of the intelligence officer, or, where appropriate, the contracted serviceman conducting the intelligence/counterintelligence activity, approved by the head of the specialised subunit.

(2) The instruction for the technical and scientific assessment shall necessarily state the factual circumstances and the questions to be answered by the specialist, with the materials to be investigated attached thereto.

Article 40. Subjects entitled to perform technical and scientific assessment

(1) The technical and scientific assessment shall be performed by specialists from the Service, or, where appropriate, the Ministry of Defence.

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

(3) Technical and scientific assessment may be ordered to professionals outside the Service or the Ministry of Defence only upon their consent on the basis of an agreement or contract.

Article 41. Organising and performing technical and scientific assessment

(1) Upon receipt of the instruction to perform the technical and scientific assessment, the head of the technical and scientific assessment subunit shall appoint a specialist having the skills and knowledge necessary to carry out the task.

(2) The specialist appointed pursuant to para (1) shall register the respective instruction and shall notify, within 3 days, whether they have the skills and knowledge to carry out the assessment.

(3) If necessary, the specialist may request additional information and materials from the intelligence officer or the contracted serviceman who ordered the assessment.

(4) After examining the materials and taking appropriate actions, the specialist shall draw up a technical and scientific assessment report expressing the opinion on the matters under assessment, explaining the facts and unclear circumstances, and establishing factual situations.

(5) The technical and scientific assessment 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 their experience in the field;

c) data on the intelligence officer or the contracted serviceman who ordered the assessment;

d) questions submitted for consideration;

e) factual circumstances;

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

g) conclusions.

Chapter V
CONTROL OF
INTELLIGENCE/COUNTERINTELLIGENCE ACTIVITY

Article 42. Parliamentary oversight

(1) Parliamentary oversight of the intelligence/counterintelligence activity shall be exercised by the parliamentary Subcommittee on Parliamentary Oversight over the work of the Service (hereinafter – *parliamentary subcommittee*), in compliance with the provisions of the Parliament's Rules of procedure, adopted by Law no.797/1996, and the Rules of procedure for the activity of the respective subcommittee, approved by Parliament's decision.

(2) The parliamentary subcommittee shall systematically inform the parliamentary Committee on National Security, Defence and Public Order with respect to its activity.

(3) Prior to the presentation, in the plenary sitting, of the annual report on the Service's activity, the Director of the Service shall submit to the parliamentary subcommittee, in closed meeting, a report on the intelligence/counterintelligence activity, which shall include, on a compulsory basis, information on:

a) the total number of counterintelligence measures ordered, carried out and rejected, for each type of measure, separately;
b) the number of initiated special files and classified special files;
c) the number of individuals notified on the performance of counterintelligence measures in their regard;
d) data on possible violations admitted by intelligence officers in the execution of the provisions of this Law.

(4) During the sitting indicated under para (3), information about completed operations performed by the Service may be presented, provided that the disclosure thereof will not prejudice the State security. The information on the ongoing operations shall not be provided.

(5) Following the presentation of the information pursuant to para (3), the members of the parliamentary subcommittee may address questions about the intelligence/counterintelligence activity carried out by the Service in the previous year. Based on the submitted information, the parliamentary subcommittee may formulate recommendations on the intelligence/counterintelligence activity of the Service.

(6) Following the examination of the information on the intelligence/counterintelligence activity of the Service according to the provisions of this Article, the parliamentary subcommittee shall take note of the submitted information and shall publish the outcomes of the oversight of the intelligence/counterintelligence activity on the official website of the Parliament, mandatorily specifying the number of the counterintelligence measures carried out by the Service, for each measure separately, as well as the number of decisions on the rejection of the approach for issuing the court warrant, for each measure separately, so as not to disclose the information assigned to state secrecy.

(7) In the event that the parliamentary subcommittee finds out that there are reasonable suspicions regarding the admission of serious violations in the intelligence/counterintelligence activity of the Service, it may request the performance of a parliamentary inquiry or may notify the Prosecutor General.

(8) The annual report on the activity of the Service shall necessarily contain a compartment on the intelligence/counterintelligence activity carried out by the Service and the measures undertaken by the Service following the recommendations of the parliamentary subcommittee.

Article 43. 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, empowered by the Prosecutor General.

(2) The control shall be carried out on the basis of complaints lodged by individuals whose rights and legitimate interests are presumed to have been infringed, or ex officio, where the public prosecutor has become aware of the infringement of the legislation related to the performance of counterintelligence measures, if such acts may constitute criminal offences.

(3) During the control performed by the prosecutor, the information on the individuals who have collaborated or collaborate confidentially with the Service may only be submitted to the prosecutor falling under the category referred to in para (1), empowered therefor by order of the Prosecutor General. The respective information shall be provided only if it is directly related to the subject matter of the control performed and only if it is absolutely necessary for the respective control performance.

(4) The prosecutors, prior to being empowered to exercise control over the counterintelligence activity, shall be entitled to the right of access to state secrecy, if they do not have such a right.

Article 44. Internal control

(1) The internal control of the intelligence/counterintelligence activity shall be carried out by the Director of the Service, the empowered Deputy Director, and, where appropriate, the Minister of Defence, including through the internal control subunits and heads of the specialised subunits.

(2) Individuals not directly involved in working with people who collaborate confidentially with the Service or the Ministry of Defence, including the Director and Deputy Directors of the Service, the Minister of Defence, shall not be entitled to request information about the real identity of individuals collaborating confidentially with the Service or the Ministry of Defence, unless this is not a matter of an urgent need at work

.

Article 45. Judicial control

The judicial control shall be performed by checking the grounds for the performance of the counterintelligence measures upon issuing the court warrant or assessing the legality of the actions carried out.

Article 46. External control over the financial means expenditure

The external control over the expenditure of financial means assigned for the performance of the intelligence/counterintelligence activity shall be carried out by the Court of Accounts, in closed meeting, pursuant to Law no.245/2008 on the state secrecy. The respective control shall be carried out within the limits not allowing the disclosure of the content, forms, tactics, methods and means of the intelligence/counterintelligence activity, identification data of individuals collaborating confidentially with the Service or the Ministry of Defence, of ongoing operations and completed operations, the disclosure of which could prejudice the security of the state.

Article 47. Control over personal data processing within the intelligence/counterintelligence activity

The processing and control over personal data processing within the intelligence/counterintelligence activity shall be carried out pursuant to the provisions of the legislation on the protection of personal data, taking into account the peculiarities of this Law.

CHAPTER VI
FINAL AND TRANSITIONAL PROVISIONS

Article 48.

(1) This Law shall enter into force in 90 days after its publication in the Official Journal of the Republic of Moldova, except for this article that enters into force on the date of its publication.

(2) Within 60 days from the date of publication of this law:

a) the presidents of the Chișinău Court of Appeal and the Supreme Court of Justice shall establish the number of judges entitled to issue court warrants and examine appeals for the

purpose of this law, shall appoint the respective judges and organise the process of random distribution of the Service's approaches/appeals;

b) the judges appointed according to the provisions of letter a) shall initiate the process of obtaining the right of access to the state secrecy, if they do not have it;

c) the Prosecutor General shall appoint the prosecutors empowered with the right of control over the counterintelligence activity.

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

PRESIDENT OF PARLIAMENT

IGOR GROSU

Chișinău, 7 July 2023.
No.179.